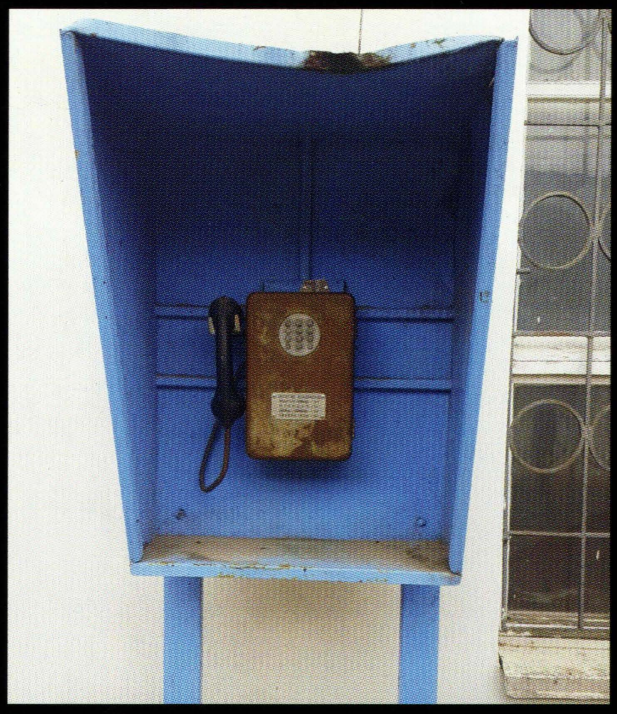
Volume Thirty-Three, Number Four
Winter 2016-2017, $6.95 US, $8.95 CAN

2600

The Hacker Quarterly

0 71486 83158 7
$6.95US $8.95CAN
64

Payphones of Europe



Russia. This ancient relic was spotted in Kostroma and has clearly seen a lot of history. It may not be sleek but it's certainly rugged.

Photo by Steve A

Armenia. Seen in Yerevan, this phone is certainly sleek but perhaps not so rugged. It's operated by the Russian company Beeline.

Photo by Simon Powell

Romania. Incredibly similar to the Armenian phone, this was discovered at the airport in Sibiu and is operated by Romtelecom.

Photo by Kevin W.

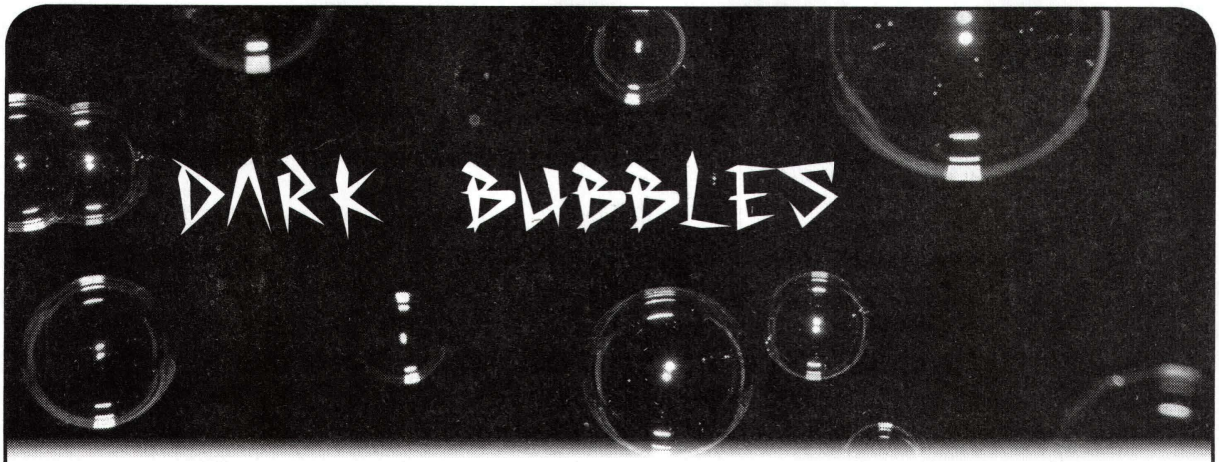
England. Found in Blackpool, this is a particularly well lit booth. It seems to have a decent color scheme going, which gives it a unique style. Best visited at night.

Photo by RykVR

Got foreign payphone photos for us? Email them to **payphones@2600.com**. Use the highest quality settings on your digital camera! (Do not send us links as photos must be previously unpublished.) (More photos on inside back cover)

Table of Contents

Dark Bubbles	4
Rescuing Fake Memory Devices	6
Having Fun with In-Store Chromecast	7
The Coca-Cola Blacklist	9
Bypassing Privileges with Oracle Database Express Edition	12
TELECOM INFORMER	13
Using Discord Servers to HTTP Flood	15
Successful Network Attacks - Phase One	16
Spying Across Borders in the Age of Email	18
InfoSec at Its Worst, OPSEC at Its Best	24
HACKER PERSPECTIVE	26
Can Security Be Built into Pure Data?	29
mcquery.js - a Web Scraper for Disc Golf Players	30
LETTERS	34
KBChat - Private, Encrypted Chat via KBFS	48
2600 Leak Department	50
Memory Lane	51
EFFECTING DIGITAL FREEDOM	52
Rotten Apples: OS X 101	54
Automatic Contest Winning via Selenium	55
The One About That File Server	57
Fiction: Hacking the Naked Princess 0x12	58
HACKER HAPPENINGS	61
MARKETPLACE	62
MEETINGS	66



If there's anything we've learned from the nonstop carnival ride our nation has been on for the past couple of years, it's that many of us spend far too much time isolated from others who have different opinions and outlooks. It can be said that this was one of the factors in the surprising election results in November. If we are to survive and make any sort of progress, this growing habit must be quelled. Since hackers always seem to be in the middle of these things, we ought to use our creativity and innovative skills to figure out solutions that usually escape the mainstream.

We all tend to hang out and communicate with people who we see eye to eye with. This makes for a more peaceful existence, with arguments and debates kept to a minimum. And that same attitude often extends to our online presence. We spend our days and nights constantly reinforcing our beliefs by trading emails and social media posts with the people who generally agree with us. We develop our Facebook, Twitter, Instagram, etc. friends and followers with this in mind. And pretty soon, we find ourselves in a virtual bubble where we feel accepted and appreciated. We're aware that there's more to the world, but we try to shield ourselves from it whenever possible.

Of course, that's not always how it turns out. Most of us have probably experienced that annoying friend or relative who somehow finds their way into our social circle and makes our life a living hell by questioning our views or countering our facts with theirs. For these situations, a variety of solutions exist with names like de-friend, block, ban, ignore, or report. Once these weapons are deployed, our bubbles become safe again.

Clearly, this approach is designed to help our sanity and preserve the peace. But it doesn't actually solve the problem; it merely puts it off. And that's kind of what happened on Election Day: all of those people who weren't communicating with each other were surprised and shocked by the outcome. Polls simply weren't able to penetrate these protective shields. And many of us realized that the country we woke up in the next day wasn't the one we had thought we were living in.

Could this surprise have been prevented? Absolutely. Communication is key and it just wasn't pursued nearly enough over the course of the campaign. And there's more than enough guilt for everyone to share here. Whether it was refusal to cooperate with the other side or simply not acknowledging their existence, we created false environments that, like any fantasy, can only go on for so long before there's a rude awakening.

As hackers, we're particularly good at seeing when something isn't quite right, despite what we may be told. When pursuing a goal or working on a project, we often discover that the path it leads us on isn't the path we originally wanted to go down. In the end, we learn things we never expected to learn and wind up with a surplus of knowledge and, often, a sense of accomplishment. Usually, the rest of the world doesn't care. To most, we waste our time in these endeavors and it becomes tiresome trying to explain them. Yet we continue to try.

This quest for information, this insatiable desire for the truth, however inconvenient, is the very definition of what a hacker is. It's a trait that is sorely needed in fields like journalism or technology of all types. So we can't be surprised when we hear that oddities in electronic voting machine results were first noticed by a group of computer scientists. In true hacker style, rather than just accept the status quo, they started asking questions. And, as with any kid who gets into trouble for asking too many questions, they were met with hostility and suspicion. But they kept at it and, within a couple

of days, over seven million dollars was raised for a recount in three states where the voting had been particularly close. It would have been easy to not put their reputation on the line or to, as so many Trump supporters delight in saying, "just deal with it." But when someone tells you to deal with something you find unacceptable, they are in effect telling you to just shut up and go away. They've been telling hackers that for a very long time and we just can't seem to get the message.

Regardless of the result (at press time, the recounts weren't finished, but we all know it's highly likely that "President Trump" will actually become a reality in 2017), we can never be bullied into submission. There is no system that can't be defeated, no set of rules that can't be thwarted with a little cleverness. A great example of this lies in our country's Electoral College system, a bizarre and antiquated relic of centuries past that allows a candidate with millions more votes to somehow lose the election. While most people favor its abolition, the means of doing that seem next to impossible, with large majorities of both houses of Congress and at least 38 states having to agree to do this within a set amount of time. Just hearing that is enough to make most people give up. But then, we heard the story of a computer scientist who stepped up to help design a possible workaround called the National Popular Vote Interstate Compact, where individual states simply agree to pledge their electors to the candidate who won the popular vote. It completely bypasses the need for a Constitutional amendment and only requires a total of 270 electoral votes from however many states sign on. They're already at 165, more than 60 percent of the way there, so this unconventional way of routing around a problem could actually work and get us past a barrier that most people believed was impenetrable. This workaround is currently being considered in Michigan and Pennsylvania and, if they agree, that number goes up to 201. As we learn over and over again, nothing is impossible with a little hacker ingenuity and alternative thinking.

But again, we can only come up with new ideas and new ways of doing things if we're open to alternative views and the possibility that we've had it all wrong. That means stepping outside of our bubbles and also moving away from the mainstream. This, also, carries a degree of risk. You've probably heard a lot of talk about something called "fake news," which allegedly played a big part in the election. In the past, it was easy to define what was "news" because it came in such limited supplies. It was also easy to control how people thought for the very same reason. Now, we have an abundance of information coming from all angles. And some of it is pretty insane, without question.

If you only get your news from people in the barbershop, you're only going to hear a particular perspective. If you turn on the TV, you'll hear something else. Add the radio, some magazines, and a bunch of alternative websites, and you've got a sizable collection of information to process and figure out. For many of us, that's too much work and so we take the easy route. That could mean never leaving the barbershop or just getting your news from your friends on Facebook, where it's easy for anything to look like legitimate news. It's believed that so many "fake news" stories were being passed around in these circles that they became the truth to many and actually helped put Trump in power under false pretenses. If true, this would be a very dangerous means of manipulation. But could the very story about "fake news" itself be an attempt at manipulation? It's certainly possible and shows why we need to always question *anything* we read. It didn't take long before we saw calls for the labeling and banning of "fake news" and, bizarrely, a list of suspicious news websites that supposedly were getting their marching orders from Moscow! While the potential damage caused by "fake news" is clear, we must also recognize the danger of entrusting anyone to tell us what is true and what is not, as truth is always subjective and prone to manipulation. This is a battle to engage in using *facts*, not a list.

If we're going to benefit from any of this, let's use this experience to encourage the questioning of everything and to start listening to the people with a whole different perspective. This doesn't mean we'll come to an agreement and start living in harmony. But at least we'll be armed with the facts and won't be living in a world that's not real. Only then are we truly equipped to fight for justice. And win.

We know the times ahead are scary for a lot of people. We feel it too. Not only will we not back down on those ideals we believe in, but we intend to become even more vocal and determined in fighting for what we see as right. Perhaps this is the environment we needed to really get things moving.

RESCUING FAKE MEMORY DEVICES

by Tau_Zer0

Part 1 - Detection

There is a scourge upon eBay and elsewhere these days: fake SD cards, flash drives, and similar memory devices. Maybe you already have one. Here's how to tell.

Method 1 - Chew Your Own Paw Off.

So you bought a memory device on eBay for a price that was too good to pass up. Perhaps 32 GB for $5. (Try to forget how silly this looks now if you're reading back issues. It was a great deal at the time.)

It says it's 32 GB. It reports that it has 32 GB. It formats successfully at 32 GB. But it has trashed some of your files.

So you test it. Write a file, read the file. OK, no problem. But the file you wrote last week is corrupt and won't read back. What gives?

Congratulations, you have a fake device. The manufacturer has perpetrated a fraud on you. The eBay (or other) vendor may be in on the con, or may be an innocent victim like you. These devices are diabolical, and can function for weeks before their true nature is known.

Here's how the con works. The device contains usually something less than one quarter of the advertised memory, but is wired in such a way as to report the full amount you "purchased." The FAT is intact, and contains entries for all the files you've written to the device, *but,* when you write beyond the actual memory area, the address lines point back and re-use earlier sectors, trashing the data they contained.

Thus your latest files are still good. As long as you stay within the first one quarter (for example) of the memory space, you're good. It's only after you take all those pictures of your recent trip to Bermuda that your earlier photos of the orgy with Beth and David get lost.

The intent of the con is, by the time you figure out that your device is just plain batty, the bloke who sold it to you is long gone.

Method 2 - H2testw.exe.

Get this Windblows executable anywhere on the Internet. It tests your memory device for its advertised memory and lets you know the scoop. No question. End of story.

Part 2 - Repair

Whoa there, don't get too exited. This procedure will *not* make your fake 32 GB device into a working 32 GB device. That would be magic - not happening.

What it *can* do is turn your useless, unreliable, can't-trust-it 32 GB garbage device into a working trustworthy 7.5 GB (for example) device.

1. Get yourself a good partition tool. Any will do. If you use Windblows and don't already have one, Paragon Partition Manager offers free trial options. [Insert standard I-don't-get-paid-for-the-plug disclaimer here.]

2. Offload and back up any files you have on the device. (Duh.)

3. Blow away all files, and then run H2testw.exe. Make note of the size of the "Data OK" area in GB. Multiply by 1024 to get MB, then knock off a couple hundred to be on the safe side. You needn't bother deleting the test files.

4. Blow away the partition.

5. Create a new partition for the number of MB you calculated, and leave the rest of the "space" unallocated. After all, it's not really there.

6. Format the partition, and then re-run H2testw.exe to verify that you have a smaller, albeit working memory device.

Part 3 - Exploitation

This section could be subtitled "Dealing With Your eBay Vendor." The first rule of eBay is, you do not enter feedback until the goods have been tested. In this case, with H2testw.

Vendors are terrified of negative feedback and will sometimes - against the rules - try to bargain with you to influence your report. Hold this Ace in your hand as long as possible. Tell them you still have it, in fact.

Where am I going with this? You might consider buying more of these devices.

Crazy as it sounds, these fake devices can actually be a good deal for the true amount of useable memory. (1) They are very cheap, especially if a vendor knows they are bad and wants

to unload them quickly. And (2), if you play your cards right, you stand a better than even chance of getting some or all of your money back.

For example, I spent about $20 for six 32 GB flash drives recently. They are really 7 GB drives. That's still not bad compared to what you would pay in a store for 8 GB drives.

I have them packed into a powered seven-port hub (cheap, eBay) where they form a six-drive RAID 5 array for my Raspberry Pi. My Pi does all my torrent processing (through a privacy VPN, of course) and I was tired of it burning out small USB hard drives from heavy use.

The six flash drives give me 35 GB of work space plus parity, and a cool light show whenever a torrent is active. And... I got my money back for the drives. A free RAID. (Performance is vastly better than a single flash drive, but I have yet to accumulate data on reliability.)

Tips when dealing with a vendor:

Be quick. Always test memory devices with H2testw immediately upon receipt.

Be polite. If the drives arrived quickly, thank him (or her) for that first, even before you complain about the quality.

Never assume he knows the devices are fake. He may have been suckered just like you, in which case you are the messenger his first impulse is to shoot. After all, you are the bearer of the bad news that his entire inventory is bogus. Have a little patience if he doesn't immediately offer you his firstborn child as compensation.

Include in your correspondence the output from H2testw, for which there is a convenient "Copy to clipboard" button.

Describe the mechanics of the con. If the vendor is dirty, he'll know immediately that the jig is up, but I've had vendors suggest that I'm putting it in the wrong way or other such nonsense. Be specific.

Mention that the cost of postage to send the device back would be more than the original purchase value.

Ask what the vendor will do to correct the situation.

He (or she - I don't mean to be sexist) may offer a partial refund. It's up to you how far to push things. You may or may not stretch the truth that you bought these device(s) in good faith (you didn't), and/or that they are entirely useless (they are not, as per the above).

The more of us who shine a spotlight on this fraud in a timely fashion, the less attractive it will be to sell these fake devices. Good luck.

Having Fun with In-Store Chromecast

by lol-md4
lol-md4@riseup.net

If you've ever used Chromecast (more generally Google Cast), you'll know how easy it is to send something (often a video) to your TV so others can enjoy. And any consumer electronics store (I'll cover Best Buy, but others are by no means exempt) will be sure to have Internet-connected TVs nowadays. So why not tap into all this potential that these TVs have?

Nowadays, Best Buy has two Wi-Fi networks (with three ESSIDs): BestBuyGuest, BBYDemo, and BBYDemoFast. All in-store "demo" devices (smartphones, TVs, laptops, etc. that are on display) are connected to either BBYDemo or BBYDemoFast; they're on the same subnet so both give you access to the same devices. The PSK for the Demo networks, by the way, is "blue1966" at the time of this writing. If this still works at your Best Buy, go ahead and skip to the "casting" section.

Getting the Wi-Fi Password via Android Devices

But what if they change it? (I sure hope they do!) Well, recall that all demo devices are connected to the same network. All of them have the password stored in plaintext, so it's clearly a secret that's very hard to keep. You'll just need to find a machine that will give you root/admin access and retrieve the password from it.

I got the current one by rooting Android devices running 4.4 using Towelroot. Since Best Buy censors `towelroot.com`, download tr.apk before you go and save it to your smartphone. You could also save it to a personal mirror or a file sharing service. When you arrive, look for the old, cheap Android devices.

Search `Settings - About Device` for the Android version and, if it's 4.4, Bluetooth tr.apk over. Now just install and run tr.apk. If it doesn't work (and you have time to wait for the device to reboot), try some of the modstrings as found on towelroot's website. I've had luck with temproot (you only need root once, after all). Otherwise, move on to another device until you root one. If you can't find any 4.4 devices (quite possible by the time you read this), you may have some luck with KingoRoot. It seems like a gimmick to me, but many have reported success with it.

Now that you have root, getting the password is the easy part. Just hit up the Play Store and search for "Wi-Fi Password" or similar. There should be an abundance of apps, but I recommend "WiFiKeyshare" because it's Free/Libre OSS. Notice that when you open the app, you will not be prompted for root access. This is because the SU binary placed by Towelroot grants all access by default. (If you used KingoRoot, you may be prompted.)

Select the Wi-Fi network all the devices in the store are connected to and hit "View Password". Good! Skip to the "casting" section below.

Getting the Password Using Windows Machines

Using Kon-Boot to get admin

No luck with the phones? Most of the Windows machines do not allow customers administrator privs, but if you do find one, skip down to retrieving the PSK below.

Meanwhile, Kon-Boot is an awesome bit of commercial software that lets you bypass login screens and escalate to admin if you have physical access. Plus, this method should work on all Windows machines. After writing it to a USB, just boot to it on the target machine. (You might have to disable Secure Boot in the UEFI settings first.) When you get to the login screen, try to login as the administrator if present or anyone else if not. Now just type literally anything (longer than 0 characters) and press Enter. If it worked, you'll be logged in.

Do `Win+R - cmd.exe Enter`. If you're in System32, cd to another directory. Do `copy C:\Windows\cmd.exe cmk.exe` followed by `cmk.exe`. If all goes well (BSODs are possible), this new command prompt is running as nt-authority\system!

Retrieving the PSK

Via the command line

Just run `netsh wlan show profile ➥ name=BBYDemo key=clear`. Find the password under `Security Settings - Key Content`.

Via the GUI

Right click on `Start` (or press `Win-X`) then open `Control Panel - Network and Sharing Center`. Click the `Connection: Wi-Fi` link. In the Wi-Fi status window, click `Properties`. In the Wi-Fi properties window, click on the `Security` tab and check `Show Characters`.

Casting Videos!

Chromecast

You're in the Demo network. Now what? Most, if not all of the TVs on the network, support Google Cast or screen mirroring. Open a supported app (*cough*YouTube*cough*), open what you want to play, and hit this button:

You'll be presented with a list of TVs/Chromecast devices to cast to. Most are named after their size (e.g. LG60L337 = 60"), so pick the largest one you can find and head to the opposite corner of the store. Pretend to shop for items and hit play!

Screen Mirroring

In case you'd like to cast an app that doesn't support Google Cast (such as a web browser), open `Settings - Display & Lights` and then scroll down to `Cast`. Check `Enable Wireless Display` in the menu and choose a device. Be careful though, as this casts your entire screen once connected. So if you're showing off an OEM theme or have icons in your notification bar, those could be used to identify you and kick you out. So perhaps you should stick to Google Cast apps. Have fun!

References and Suggested Material

- Towelroot: `https://towelroot.com`
- modstrings: `https://towelroot.com ➥/modstrings.html`
- KingoRoot: `https://www.kingoapp ➥.com/`
- Kon-Boot: `http://piotrbania.com ➥/all/kon-boot/`
- Big Bill Hell's, a pretty fun video to blast: `https://youtu.be/4sZuN0xXWLc`

You could also go for something more subtle, like a nature slideshow dubbed with an extremist podcast, for example.

The Coca-Cola Blacklist

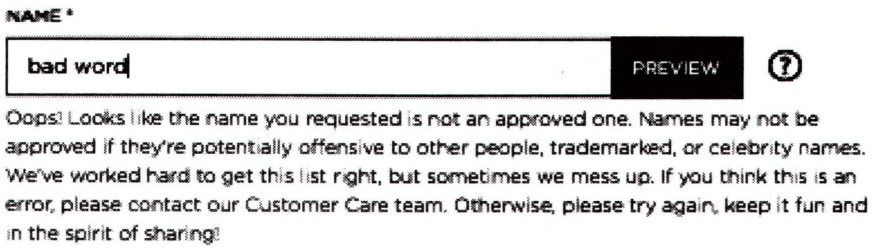
by Dent

Some of you may already be familiar with the Share A Coke campaign. The 2015 summer promotion was an immediate success, selling roughly 250 million bottles of Coca-Cola by using generic names such as "Mark" or "David" instead of the usual Coca-Cola logo. Then, sometime in 2016, they introduced personalized bottles for people with more unusual or complicated names by using an online form and ordering application. This also resulted in the creation of a blacklist, or a list of terms that Coca-Cola does not allow you to put on bottles. This list includes trademarked names, political leaders, celebrities, profanity, and sometimes just plain old random things.

As of a few weeks ago, I've begun collecting what terms the online form will and will not allow me to print on bottles. Some of these terms are unbelievably vague, and many very offensive terms are unbelievably allowed. Things like the letters of the alphabet (except for G and N), the most common name in the world (Mohamed), Donald, Hillary, Hacker, and Phreak are all examples of forbidden names. The list actually contains the term "Coke" even though it's in the damn slogan! After a few solid days of trial and error using various online dictionaries and consulting a few creative friends, a large list of banned terms was generated.

What's even more interesting is how easy it is to bypass blacklist detection. It doesn't involve any special homoglyphs or alternate spellings. Simply adding a space before or in between terms allows for anything to be used as a valid, non-blacklisted term. This doesn't stop human moderators from canceling orders, so you obviously won't be drinking a "Share a Coke with Hitler" bottle any time soon. It does, however, allow you to order bottles for friends whose names are blacklisted for no good reason.

While I've found many terms to add to this blacklist, there are many more waiting to be found. To find a blacklisted term, navigate to `https://buy.shareacoke.com/personalized-➥bottle/` and use the provided textbox to type in any terms that could be blacklisted. If you receive the error message pictured below, it's on the blacklist!


NAME *
bad word
PREVIEW
Oops! Looks like the name you requested is not an approved one. Names may not be approved if they're potentially offensive to other people, trademarked, or celebrity names. We've worked hard to get this list right, but sometimes we mess up. If you think this is an error, please contact our Customer Care team. Otherwise, please try again, keep it fun and in the spirit of sharing!

The above error message is not at all uncommon. In fact, "Bad word" isn't just an example. It's really on the list!

The following list contains every term that I and others have tested, and is in no way, shape, or form the complete list. This list contains many controversial and outright horrible words, however, these words are not written to provoke, but to understand. Terms that might arouse particular interest are bolded for your convenience.

BLACKLIST

0 (this number is really blacklisted)
A (this letter is really blacklisted - not a category)
Adolf
Adolf Hitler
AK47
Allah
Aloha Snackbar
Al Qaeda
Al-Qaeda
Anus
Apple
Armed
Army
Arse
Ass
Assclown
Ass clown
Assface

Ass face
Asshat
Asshole
Ass hole
Asswipe
Autism
B (this letter is really blacklisted - not a category)
Bad word
Balls
Barack Obama
Bestiality
Bisexual
Bin Laden
Bitch
Bitchass
Bitch ass
Bitches
Blacks
Blood
Bloods
Blowjob
Bollocks
Bomb
Bomber
Bombs
Boner
Boob
Boobs
Boogieman
Booty
Brown
Buda
Budda
Buddhism
Buddhist
Bullet
Bullets
Bunghole
Butt
Buttfuck
Buttplug
Butts
C (this letter is really blacklisted - not a category)
Carpetmuncher
Chainsaw
Chode
Clinton
Clit
Clusterfuck
Cocaine
Cock
Cockhead
Coke (really?)
Coochie
Coon
Cooter
Cracker
Cum
Cunnilingus
Cunt
Cuntface
Cunt face
D (this letter is really blacklisted - not a category)
Damn
Dank Memes
Darth Vader
Dick
Dickface
Dick face
Dickhead
Dick head
Dicks
Dicksuck
Dick suck
Dildo
Donald
Donald Duck
Donald J. Trump
Donald Trump
Dookie
Douche
Dr who (Dr Who works fine)
Dr. Pepper
Dum
Dumbass
Dumbfuck
Dyk
Dyke
Dykes
E (this letter is really blacklisted - not a category)
EA
Ew
Extremist
F (this letter is really blacklisted - not a category)
Facebook
Fag
Fagbag
Faggot
Faggots
Fags
Fanta
Fart
Farts
Fat
Fatt
Fatty
Fattie
FBI
Fellatio
Feltch
Flamer
Fuck
Fucker
Fuckers
Fuckboy
Fuckface
Fuck face
Fuckoff
Fuckwad
Fudgepacker
Gay
Gays
Glock
God
Google
Gook
Gun
Guns
H (this letter is really blacklisted - not a category)
Hacker
Handy
Handjob
Harambe
Hell
Hillary
Hillary Clinton
Hispanic
Hitler
Ho
Hoe
Holocaust
Homo
Homos
Honkey
Hump
Husain
Husayn
I (this letter is really blacklisted - not a category)
Idiot
Idiots
Indian
Indians
Iraq
Iraqi
Irony (thanks Enamon)
Islam
J (this letter is really blacklisted - not a category)
Jackass
Jagoff
Jap
Jerk
Jerkoff
Jerk off
Jesus
Jesus Christ
Jew
Jews
Jihad
Jizz
Judaism
K (this letter is really blacklisted - not a category)
Kootch
Kickass
Kike
Kim Jong Un
Kim Jung Un
Kindle
KKK
Ku Klux Klan
L (this letter is really blacklisted - not a category)

Lame
Lesbian
Lesbians
Lesbo
Lezzie
Losers
M (this letter is really blacklisted - not a category)
Marijuana
Mahamed
Mahammed
Mcfaggot
Meth
Midget
MILF
Minge
Mohamed
Mohammed
Moobs
Moses
Mothafucka
Motherfucker
Muff
Muffdive
Muffdiver
Muhamed
Muhammed
Mummie
Murder
Murderer
Muslim
Name
Nazi
Negro
Negroes
Nig
Niga
Nigga
Niggas
Nigger
Niggers
Niglet
North Korea
NSA
Nut
Nuts
NWA
O (this letter is really blacklisted - not a category)
Obama
Osama bin Laden
Osama bin Ladin
P (this letter is really blacklisted - not a category)
Pedophile
Pee
Penis
Pepsi
Phreak
Piss
Pistol
Poison
Poo
Poon
Poontang
Poop
Poopie
Poopoo
Poopy
Poo-poo
Prick
Prostitute
Protest
Pus
Pussy
Putin
Puto
Q (this letter is really blacklisted - not a category)
Queef
R (this letter is really blacklisted - not a category)
Rape
Rapist
Retard
Retards
Rifle
Rimjob
Rum (thanks Enamon)
S (this letter is really blacklisted - not a category)
Sand nigger
Sarcasm (thanks Enamon)
Satan
Satanism
Schlong
Scrot
Scrote
Sex
Sexy
Shit
Shitbag
Shithead
Shit head
Shithole
Shit hole
Shits
Shitting
Shitty
Skank
Skeet
Slut
Sluts
Snatch
Soldier
Spook
Spooks
Sprite
Stalin
Starbuck
Starbucks
Star Wars
Suicidal
Suicide
T (this letter is really blacklisted - not a category)
Taliban
Tard
Terror
Terrorist
Testical
Thundercunt
Tit
Tits
Tittie
Titty
Trump
Twat
Twats
U (this letter is really blacklisted - not a category)
Unhealthy
V (this letter is really blacklisted - not a category)
Vagina
Vaj
Vajayjay
Virus
Vladimir Putin
W (this letter is really blacklisted - not a category)
Wank
War
Weed
Wetback
Whore
Whorebag
WWI
WWII
X (this letter is really blacklisted - not a category)
XXX
Y (this letter is really blacklisted - not a category)
Yahoo
Z (this letter is really blacklisted - not a category)
Zoolander

Bypassing Privileges with Oracle Database Express Edition 11g Release 2

by Chris Rucker, Data Scientist

The basis of this project was to create a link between two disparate database servers in order to cross validate row counts. Oracle Database Express Edition 11g Release 2 is described as an "entry-level, small footprint RDBMS" based on its big brother Oracle Database Edition 11g Release 2. Oracle Database Express Edition (XE) addressed the immediate need by myself to compare the record counts of like tables loaded from different networks where I did not have sufficient privileges to build database links. The idea was to introduce an SQL *minus* script into XE subtracting the rows of one table in server A from its counterpart in server B or vice versa. Upon completion of the project, I found that I could bypass certain DBA-enforced rules simply because I was sitting behind the network and using a free third-party database server, namely XE.

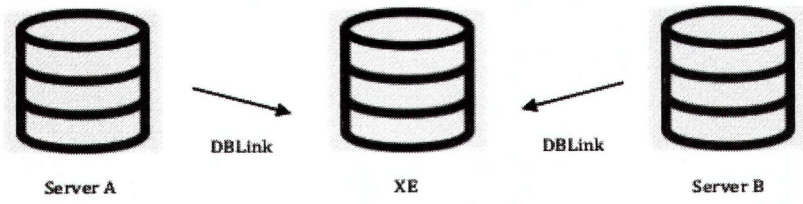
Firstly, I downloaded and installed XE from Oracle's website. You may need an account, but that is pretty easy to obtain. And installation is similar to installing other databases in terms of the tnsnames.ora file, etc. I used SQL*Plus to access XE from a Windows CLI with a system name and password similar:

```
sqlplus system@xe/oraclexe
```

Secondly, I established links to the two disparate databases once XE was up and running similar:

```
create public database link <alias A>
connect to <owner A>
identified by <password A>
using '<server A>';
create public database link <alias B>
connect to <owner B>
identified by <password B>
using '<server B>';
```

So XE now sits between server A and server B which are linked together by database links.



And now I can run my minus scripts and spool them similar:

```
select <columns>
from <tables>
where <conditions>
minus
select <columns>
from <tables>
where <conditions>
```

I received an "ORA-01031: insufficient privileges" error upon trying to establish a public database link in server A to server B which made it impossible to run the minus script and perform cross validation. So, installing XE and creating the links on XE bypassed any database administrator privileges that I might normally need to make the two databases shake hands.

The second unexpected benefit of running XE was the ability to run subroutines like procedures, functions, and triggers after creating copies of tables from server A/B on XE similar:

```
create table <table> as
(select * from <schema><table>@<dblink>);
```

Lastly, Oracle Database Express Edition 11g Release 2 allowed me to create database links, run my scripts, and create procedural language (i.e., PL/SQL) where I ordinarily would have encountered "insufficient privileges" errors. Not bad at all for a free database.

TELECOM INFORMER

by The Prophet

Hello, and greetings from the Central Office! Or, in this case, the Central Fancy Lounge. I am writing to you from Vancouver, where I'm en route to Hong Kong and then onward to Myanmar. I managed to social engineer my way into the first class lounge and, soon, I'll be winging my away across the Pacific in - *somehow* - a first class seat. Given that I spend most of my time on the road in Seat 31B, it's a nice change. They literally serve champagne and caviar and it's not even in a heavily ironic sense. Naturally, I dressed up for the occasion, picking my least battered cargo pants and tennis shoes for this one. The staff are visibly appalled and are doing their best to ignore me.

I love to visit Vancouver. It has always been a wonderful, cosmopolitan city (apart from the disgusting Automatic Electric EAX switches still in use by Telus). In fact, it's so civilized that mobile phones even work underground on public transportation! Every time I come to Canada, though, I grit my teeth. Why? I have a long-term telephony problem that hangs like an albatross around my neck.

Ten years ago, I took a vacation to Newfoundland. Back then, my mobile phone provider was Sprint, and they had no reasonably priced way to roam in Canada. I forget exactly what they charged, but it was something ridiculous like $1 per minute plus long distance. And there was no data service available at all; only voice and text were offered. So naturally, I picked up a Virgin Mobile Canada Nokia 6015i and promptly set about hacking the WAP stack. All I had to do was change the DNS server to an outside one (I used Sprint's) while in debugging mode and I was able to browse the mobile web for free for my entire trip, making the $50 I spent on the phone and $20 for the recharge a good investment. Better yet, using a data cable, I was able to tether! 14.4Kbps mobile Internet in my tent while camping near Gros Morne National Park, and I was in seventh heaven. I must have used at least 50MB of data on my trip, which back then was a lot. Not surprisingly, Virgin Mobile noticed my shenanigans and fixed the problem not long after that.

Well, you know what happens next. What started as a $20 prepaid balance has grown over the years to being a balance of over $1,000. Why? There is no monthly fee at all if you have a British Columbia phone number, so the only thing that drains the balance is voice minutes and SMS. All that I have to pay is $100 per year to keep the service active (which applies as a credit to my account). Naturally, I didn't want to lose the $20 balance I had after I returned from Newfoundland, so a year later I paid $100 to keep it, and have just been putting another $100 per year on my account ever since.

Virgin Mobile Canada is a Canadian MVNO, but an unusual one in that it is owned by Bell Canada. Over the years, Bell has acquired most of the Canadian mobile phone networks on which it operates, so I'm not sure whether it can properly be called "virtual" anymore. Originally sold as a "pay-as-you-go" service (and this is the grandfathered plan I still have), it's like a mobile phone plan out of the 1990s except that it's still available today. Minutes cost 30 cents each, long distance calling (remember long distance?) is charged at 30 cents per minute on top of that, and if you receive a call in a different region than that where your phone number is based, you pay for forwarding the call from your home region. Despite the high charges, I bring my trusty and increasingly dated Nokia 6015i on every visit to Canada and valiantly attempt to use a few voice minutes or send a couple of texts. The phone has long ago ceased to be useful for anything on the Internet whatsoever, with WAP being a long-forgotten standard and 14.4Kbps unable to keep up with essentially anything online. My T9 skills are no longer relevant in a world of touch-screen smartphones.

Still, the Nokia was like a comfortable pair of old shoes. I say "was" because today I had to give it up. A couple of months ago, I received notice from Virgin Mobile Canada that I needed

to switch to an LTE phone or risk my service being suspended. When I called, nobody was really sure what would happen if I didn't switch, but nobody was willing to guarantee that I wouldn't lose the balance either. With over $1,000 (CAD) at stake, that was too big a risk, so I decided not to experiment with telephony disobedience.

Canadian mobile phone carriers have taken a dramatically different approach than U.S. carriers to the retirement of CDMA2000, a standard that increasingly lacks relevance in the world of LTE. Developed by Qualcomm, CDMA IS-95 2G networks (and later CDMA2000 3G networks) were designed as a smooth network migration path to digital from analog. These supported the use of an ESN/MIN pair, meaning that billing systems didn't have to be upgraded. In fact, phones could support both networks with the same ESN/MIN pair and be billed identically regardless of the technology used. This allowed carriers to roll out digital networks slowly while still maintaining good coverage with their existing analog networks.

Of course, the tradeoff was that this standard was incompatible with the GSM digital standard used in the rest of the world. That tradeoff was unacceptable to some carriers, particularly cost-conscious ones (GSM network equipment was less expensive). In Canada, Rogers Wireless opted to switch its customers to GSM, eventually retiring its AMPS analog network entirely. AT&T took the same approach in the United States. However, almost every other carrier opted to go with CDMA. In the U.S., the companies that eventually became Verizon did the same, along with U.S. Cellular.

"PCS" carriers, with no legacy networks to support, were about evenly split in the technology chosen. At the time that these networks were built, CDMA offered faster data speeds and "soft handoffs," which offered a better customer experience than GSM. Call quality was better, and network operators could also offer roaming on legacy analog networks. This attractive combination spurred Sprint, Cricket, metroPCS, and many other PCS carriers in the U.S. (along with Bell in Canada for the PCS coverage it built) to choose CDMA. In the U.S., VoiceStream (which later became T-Mobile) chose GSM, and Fido did the same in Canada.

The direct upgrade path to IS-95 CDMA was CDMA2000. However, this was immediately challenged by UMTS, the successor to GSM. UMTS (later followed by HSDPA) was a CDMA technology offering all of the advantages of CDMA2000 along with faster speeds and better features. Although CDMA2000 doesn't support phone calls and data usage at the same time, UMTS and HSDPA did. Along with this, they had backwards compatibility with GSM and its massive globally deployed userbase.

This started to create a problem for carriers that had adopted CDMA2000, because they couldn't get the best handsets. It all came to a head with the launch of the iPhone. Apple decided to launch with AT&T, and they bet big on GSM and its successor technologies. This wasn't done in a vacuum. Outside of North America, CDMA never really caught on, while GSM adoption exploded. A handful of carriers used CDMA (Telecom New Zealand, China Telecom, and Iusacell in Mexico), but almost none of them were the dominant providers in their respective markets. GSM marched across Europe, Asia, Africa, and South America. Europe even mandated GSM compatibility by law.

The writing was on the wall, so Canadian CDMA carriers - unlike their U.S. counterparts - began deploying HSDPA and UMTS on their towers alongside CDMA2000. In 2009, Telus soft launched HSDPA in Canada, giving its customers access to the latest handsets. In 2012, Telus stopped selling any handsets with CDMA support, so any customer forced to upgrade has a handset at least five years old. Meanwhile in the U.S., CDMA carriers stuck with CDMA2000 and waited for 4G WCDMA technologies to emerge before making major network upgrades. In fact, Verizon and Sprint still sell handsets with CDMA2000 support. While CDMA will eventually be retired in the U.S., Verizon has committed to supporting the technology through at least 2021.

So, that's why I just paid $5 for a new Virgin Mobile SIM card. And with that, it's time for me to "enjoy" it and call some Canadian friends. I have a modern phone supporting nearly all of the latest technologies, a 4G LTE SIM card, and a mobile phone plan that is a relic of the 1990s. However, it's one that I'll hang onto with a death grip as long as there is no monthly fee!

Enjoy your winter, and try to use a CDMA network while you still can. As of January 31, 2017, you won't be able to do so in Canada. Try to be the last call.

by xnite

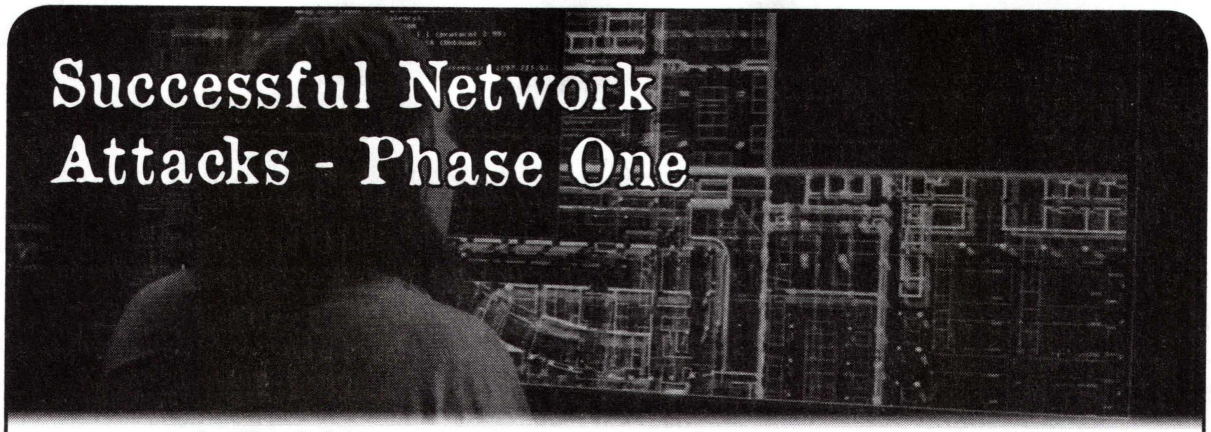
In October, I decided to check out a possible flaw in Discord, a popular voice/text chat application that can be run in the web browser. Since the service uses a scanner to scan links posted in chat, I wanted to check if that scanner could be used to launch a denial of service attack. As things would have it, you can post multiple variations of links in a single message and, for each time, Discord will make a request to that link. On average you can post the link about 20 to 50 times in a message, and roughly four messages per second before rate limiting kicks in. In theory, a single client can send a maximum of 50*4 requests per second (200 requests per second) as long as you use a different variation of the link each time (i.e., https://example.com/image.png?id=1, https://example.com/image.png?id=2, etc. This doesn't sound like a lot, sure, but there are some fairly potent methods of DoS out there that we can utilize here to make this a nasty attack. A very effective DoS method to use against WordPress is to send randomized search requests to a website, so this is what I will be talking about and testing against.

Before I begin, here's a primer on the WordPress issue. With WordPress, you can make search requests by grabbing up /index.php?s=# where # is your search term. To leverage search for a DoS attack all you need to do is flood it with many requests for random terms. This method bypasses caching on the website and MySQL server alike. The attack causes stress on not only the web server, but the MySQL server too. This method also tends to pass right through Cloudflare making it an ideal choice for this Discord DoS attack.

Utilizing the Discord API, I wrote a bot that would wait for commands on any Discord server it is invited into. The bot leverages the URL scanner on Discord to make requests to the given target website by making a bunch of requests in single messages to flood out the URL scanner. The bot takes the command "!poc U L R". U represents the base URL (e.g. https://example.com/index.php?s=), L represents the number of loops (per bot), and R represents the number of requests per message. The command might look something like this "!poc https://example.com/index.php?s= 10000 30". With multiple bots running, you can make 4*(B*R) where B represents the number of bots, and R represents the number of requests per message. If you have fove bots, each making 50 requests per message, you would be making 4*(5*50), or 2,000 requests, per second. With only five bots, I was able to take down my test WordPress installation in its default configuration, on an Nginx web server, also with default configuration including WordPress configuration. Unfortunately, I'm fairly certain wordpress.com sites are protected from this sort of attack, but then again I haven't tried it.

My proof-of-concept source code will be available at `https://gitlab.com/xnite/harmony` as soon as this issue is published. If you have any questions, comments, or concerns, you can open an issue there.

Successful Network Attacks - Phase One



by Daelphinux

Network attacks are a common threat in the modern world. Businesses, affiliations, community organizations, and even individuals are at risk to these kinds of dangers. While the attacker may have any number of motivations, the attacks are often carried out in similar ways. Successful attackers must be dedicated and committed to the attack they are attempting to carry out. Moreover, they must be diligent in successfully completing each of the five phases of a network attack.

These phases are considered common knowledge in the security fields:

Phase 1: Reconnaissance - Gathering as much useful information about the target as possible.

Phase 2: Scanning - Gathering useful information about the target's networks and any possible exploits.

Phase 3: Gaining Access - Getting into the network to be able to accomplish the attack's goal.

Phase 4: Maintaining Access - Ensuring access to the network persists long enough to accomplish the attack's goal.

Phase 5: Covering Tracks - Obfuscating the attacker's presence on the network such that they cannot be traced.

Each of these phases is critical to the success of an attack. They form a kind of pyramid where each step builds upon the success of the previous one.

With poor reconnaissance, a network scan is unlikely to have the proper information necessary to ensure that accurate loopholes and useful exploits can be found. With a bad network scan, it is unlikely that access will ever be gained. With no gained access, there is no access to maintain, and if there is never any access, there are no tracks to be covered.

Additionally, each phase has various processes and skills necessary to achieving the end result. A successful attacker will have to understand all of these processes and skills; conversely, a successful defender will have to understand them just as well. Understanding the methodology of an attack will allow a defender to stay one step ahead of an attacker, but just like an attack will fail with a single misstep, so will a defense. Security professionals must be vigilant to watch for signs of oncoming attacks, learn to recognize each phase, mount a defense against each phase, and contingently prepare for failing to prevent each phase.

For each phase, there will be an overview of what occurs during the phase, a view on how to recognize the phase, defend against it, and prepare for failing to defend. Further, scenarios will be given that will allow a defender to know exactly what to expect is going on with the attacker's end. Once a security professional understands how to recognize each phase, they will be able to apply that information in aggregate to recognize when an attack is likely to be coming; however, truly predicting that is a combination of luck and experience.

Phase One: Reconnaissance

In order to do anything successful in a given setting, knowledge of the tasks and obstacles that may prevent the task is crucial. After determining an end-goal for the attack, such as gathering user data from a target, the first real step in the attack process is to gather useful information about the target. "Useful" is a very important word here. During the reconnaissance phase, a wealth of useless information will, inevitably, be gathered. It is important to be able to filter out the junk information and retain the useful information, although it is unlikely one will be able to perform that filtering on the spot.

In this phase, the attacker will likely be gathering information from every source

imaginable. They will be running deep web searches, calling public phone lines, checking the whois entries of any of the target's domains, launching social engineering attacks (things such as phishing, email scams, prodding users for information, and even making new friends), and going so far as to dive through dumpsters for improperly disposed of documents. This will leave the attacker with a giant wealth of information. Most of it will be completely and utterly useless. Within that overbearing mountain, however, a skilled attacker will be able to gather information that will be extraordinarily useful. A couple of stray printer configuration pages, a list of email addresses, or some network shares written down on scraps is invaluable in this phase of an attack.

An attacker will be looking for anything that gives them clues regarding the target's:

- network information (subnets, IP ranges, VLANs, etc.)
- manufacturers of computing equipment
- printer manufacturers
- internal organization
- operating system versions
- network equipment manufacturers
- username policies
- password policies
- and more

This information will give the attacker what they need to determine if any known exploits exist for the target's systems and begin formulating a plan to look for unknown exploits.

It is very difficult to recognize the reconnaissance step of an attack. Security footage or reports of dumpster divers can be a good clue, but even those aren't necessarily indicative of an incoming network attack. Those could be completely innocuous situations where a person is trying to reap usable hardware with no desire for any data, or even someone down on their luck just trying to score a meal. The rest of the methods commonly used for reconnaissance are almost impossible to detect as being malicious, as they are not really any different than the day to day actions of a normal end-user.

However, while this is the most difficult phase to detect, it is the easiest to defend against. The flow of useful information is paramount to the attacker's success in Phase One; the easiest solution is to cut off the flow of information. Some pieces of useful data cannot be denied: Whois information, addresses of company buildings, any publicly available phone numbers, or even basic website information and email addresses will always be able to be accessed. However, ensuring on-site security and destruction of purchase order information, manufacturer manuals, boxes for critical equipment, and anything bearing network information (server names, IP addresses, etc.) up to and including things as seemingly innocuous as printer configuration pages can make a world of difference in an attack.

Employees and other associates should be instructed to destroy certain documents once their purpose has been fulfilled. In most cases, simply shredding a document with a cross-cutting shredder will suffice. However, for particularly sensitive information, it may not be a bad idea to maintain burn storage for documents that will need to be burned, in most cases, by an off-site solution. Although this includes a third-party in the security process, with proper vetting and research, a reputable third-party destruction solution is often a more cost-effective route.

Although these steps prove to be very easy to plan in theory, they are much harder to implement in practice. Ensuring that information never leaves the facility places a requirement on end-users, service employees, and executives that may or may not be fulfilled. Company policies do a lot to promote good practice, but human nature tends to work against that. Mistakes are made, lazy practices exist, and sometimes it comes down to forces of habit. If employees are used to simply throwing documents away instead of destroying them, it may be difficult to retrain them to perform a different task.

However implemented, the goal of a Phase One defense is to prevent the flow of useful information. Even better is to implement a plan that prevents the flow of *any* information, but that is, alas, unrealistic. It would not be cost effective in most environments to destroy or prevent any information that would otherwise leave the facility when comparing the benefits to the risk. However, in ultrahigh security situations, this solution has proven to be viable.

Should a well-formed defense fail against a Phase One attack, it is likely that a Phase Two attack would be incoming. The best preparation for the failure of a defense against all but two of these phases directly correlates to successfully defending against the next phase, the exceptions being Phase Three and Phase Five, which will be addressed in their appropriate sections.

Spying Across Borders in the Age of Email

by Rodrigo Ruiz and Rogério Winter
rodrigosruiz@outlook.com,
rogwinter@gmail.com

In times where the opponent was a state, as during the Second World War, all efforts were made to ensure secure communication. The Germans had the Enigma code, while the Allies came to use pigeons to cross the lines with vital information. During the war itself, the Allies deciphered the German encryption machine, beginning a real obsession with how to decode ciphers of the opponents and, at the same time, create powerful ciphers for their own use.

The pigeons have been replaced by emails. Today, instant messages are the most common form of communication between companies, individuals, and governments. Large distances are overcome with a simple click of the mouse, permitting all kinds of research in collaboration with colleagues around the world. But to what extent are we safe? In that fraction of a second between sending and receiving messages via email, who else will have access to them? In response, service operators include guarantees within their contracts about user privacy, along with the use of SSL[1] to protect communications.

The persona of the spy, popularized by James Bond 007, is also associated with real-life versions of the National Security Agency (NSA) of the United States of America[2], the CIA[3], and the extinct KGB (FSB)[4]. Meanwhile, the Edward Snowden case[5] has resulted in geopolitical consequences for, as well as caused discomfort and financial damages among, former allies as evidence that espionage on a large scale is no longer limited to the declared enemy. After 9/11, the game of espionage changed again. Fear changed the way of life around the world. Privacy and confidentiality are characteristics, which, when lost, result in financial losses and demand a considerable effort to regain them, although recovery is virtually impossible. This issue is well characterized by Bruce Schneier[6]. Society has opened up its privacy in exchange for the promise of more security. Who decides which particular individual should be the focus of monitoring focus, and in what form? In January 2015, the magazine *Science* published a special issue titled "The End of Privacy"[7].

Large companies are often blamed for providing data on people and institutions indiscriminately to governments without appropriate legal actions. As there are no effective means of control, businesses and individuals essentially depend on the trust that people have in these large companies that hold records on us.

On the 11th of July 2013, the British newspaper *The Guardian*[8] published the contents of top secret documents, showing that Microsoft works in conjunction with the NSA and the FBI, helping these agencies to circumvent new encryption procedures in its products, including Outlook.

Microsoft was given the right to reply by the newspaper: "We have clear principles which guide the response across our entire company to government demands for customer information for both law enforcement and national security issues. First, we take our commitments to our customers and to compliance with applicable law very seriously, so we provide customer data only in response to legal processes."

The Game's Afoot

In January 2015, during a routine check, we found evidence that an email account linked to our research had been accessed without authorization. Despite our indignation towards this breach in our email security, rather than scare the hacker, we decided to exploit the situation and expand our knowledge of email privacy.

During the first months of 2015, email communications were made using controlled messages in order to protect the integrity of our research, while our curiosity about the hacker continued to increase. By monitoring the situation, we obtained an Outlook access report (see Figure 1). As can be seen in Table 1, IP address properties were established through consultations with ARIN[9] and RIPE.net[10] (see Figure 2).

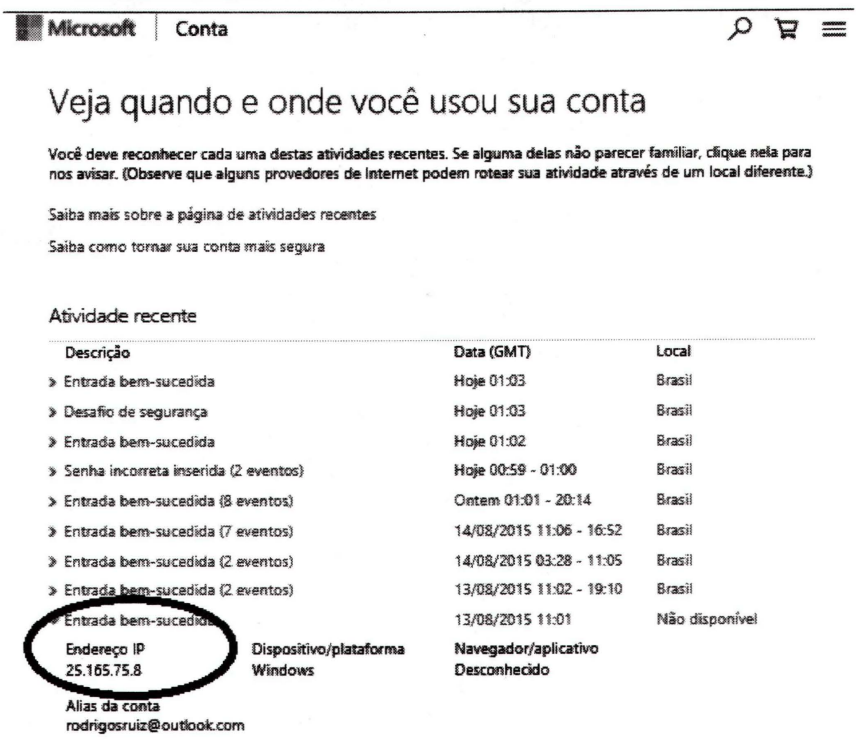


Figure 1. Microsoft Outlook access report and IP 25.165.75.8, which is the property of the UK's Ministry of Defence.

Date/time	IP	Owner	Local
15/01/2015 13:22	157.56.238.188	Microsoft Corporation	Redmond
29/01/2015 14:39	132.245.80.92	Microsoft Corporation	Redmond
02/02/2015 04:10	132.245.32.12	Microsoft Corporation	Redmond
02/02/2015 04:10	132.245.32.11	Microsoft Corporation	Redmond
03/02/2015 04:49	132.245.11.4	Microsoft Corporation	Redmond
03/02/2015 14:15	132.245.32.4	Microsoft Corporation	Redmond
09/02/2015 12:15	198.11.246.181	Softlayer/F-Secure	Chantilly/ Washington
20/03/2015 10:41	25.163.90.11	Ministry of Defence, UK	London
20/03/2015 16:46	25.160.164.153	Ministry of Defence, UK	London
31/07/2015 20:04	25.165.74.23	Ministry of Defence, UK	London
13/08/2015 11:01	25.165.75.8	Ministry of Defence, UK	London
30/10/2015 09:24	25.165.118.133	Ministry of Defence, UK	London
27/11/2015 11:28	25.165.74.25	Ministry of Defence, UK	London

Table 1. List of IP addresses through which the email account was improperly accessed.

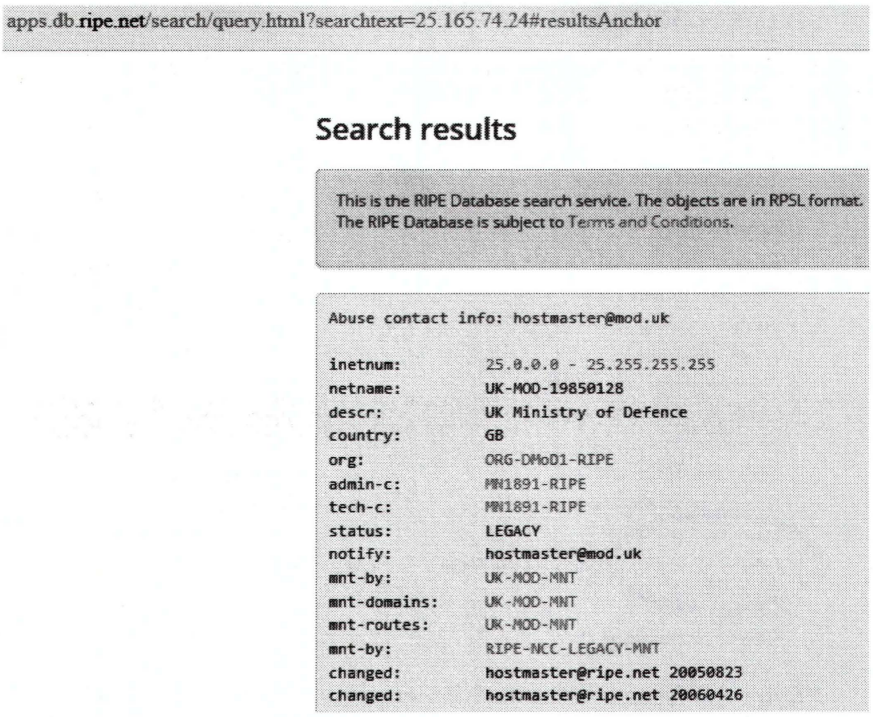
The password used to protect the account assigned at the time of the incidents was regarded as "strong," that is, it contained a great number of numbers, upper and lower case letters, and special characters, which is a format typically used in IT (e.g. "f5Gr$ekslanhjo").

It would be unthinkable that a corporation, which is one of the symbols of America, would be institutionally involved with an unfriendly foreign government.

During recent years, the entire world's media has regularly referred to the NSA in the context of any espionage action, control, and invasion of privacy against people, businesses, and governments around the world.

These reports have also shown that there is at least another player in the game - the UK - as seen in Figure 2, Figure 3, and Table 1. The evidence, which is indisputable, points to actions of the UK in the USA, specifically in Microsoft. In the search for an answer, we contacted the UK's Ministry of Defence[11], who were evasive in response, as can be seen in Figure 3. When the UK

government answers by saying, "We do not confirm and we do not deny," it alerts everyone to the privacy and security of the UK's business, industrial, and scientific secrets.



apps.db.ripe.net/search/query.html?searchtext=25.165.74.24#resultsAnchor

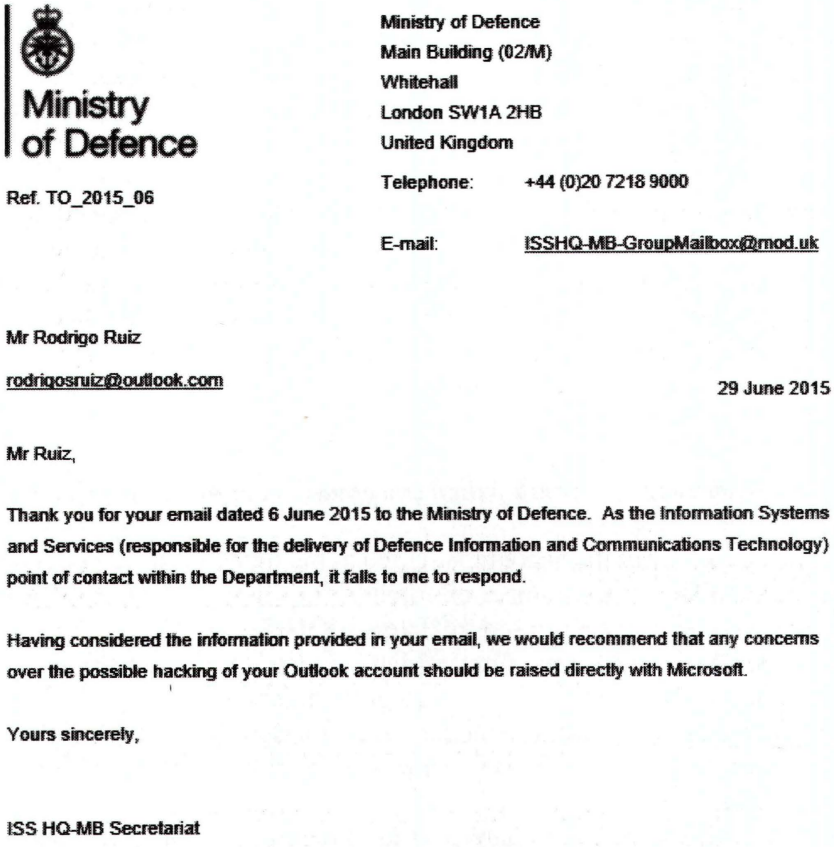
Search results

This is the RIPE Database search service. The objects are in RPSL format.
The RIPE Database is subject to Terms and Conditions.

```
Abuse contact info: hostmaster@mod.uk

inetnum:        25.0.0.0 - 25.255.255.255
netname:        UK-MOD-19850128
descr:          UK Ministry of Defence
country:        GB
org:            ORG-DMoD1-RIPE
admin-c:        MN1891-RIPE
tech-c:         MN1891-RIPE
status:         LEGACY
notify:         hostmaster@mod.uk
mnt-by:         UK-MOD-MNT
mnt-domains:    UK-MOD-MNT
mnt-routes:     UK-MOD-MNT
mnt-by:         RIPE-NCC-LEGACY-MNT
changed:        hostmaster@ripe.net 20050823
changed:        hostmaster@ripe.net 20060426
```

Figure 2. The RIPE Network Coordination Centre, the organization responsible for coordinating IP registries in Europe, assigns the range 25.0.0.0 to 25.255.255.255 to the UK's Ministry of Defence.



Ministry of Defence

Ref. TO_2015_06

Ministry of Defence
Main Building (02/M)
Whitehall
London SW1A 2HB
United Kingdom

Telephone: +44 (0)20 7218 9000

E-mail: ISSHQ-MB-GroupMailbox@mod.uk

Mr Rodrigo Ruiz

rodrigosruiz@outlook.com

29 June 2015

Mr Ruiz,

Thank you for your email dated 6 June 2015 to the Ministry of Defence. As the Information Systems and Services (responsible for the delivery of Defence Information and Communications Technology) point of contact within the Department, it falls to me to respond.

Having considered the information provided in your email, we would recommend that any concerns over the possible hacking of your Outlook account should be raised directly with Microsoft.

Yours sincerely,

ISS HQ-MB Secretariat

Figure 3. Response from the UK's Ministry of Defence when asked if it authorized the intrusion into the researcher's email account or whether its own computers had been hacked by third parties, thereby allowing access.

When questioned about these incidents, Microsoft[12] provided the following protocols: `1076B89D; 9023A4AE; 4FB0DD02; B860A2E9; 102FD43B.`

On the 18th of December 2015, Microsoft Computer Emergency Response provided the reply as shown in Figure 4. When Microsoft declared that the access simply involves a Microsoft server-to-server call, we might ask the following:

1. Are Microsoft Outlook servers embedded in the UK's Ministry of Defence infrastructure? If so, why?

2. In Figure 6, we present an example of human interaction in Washington DC in which a user typed in a wrong password a few days before London received access to the email account. Why would Microsoft imagine that an automated server system would type in wrong passwords?

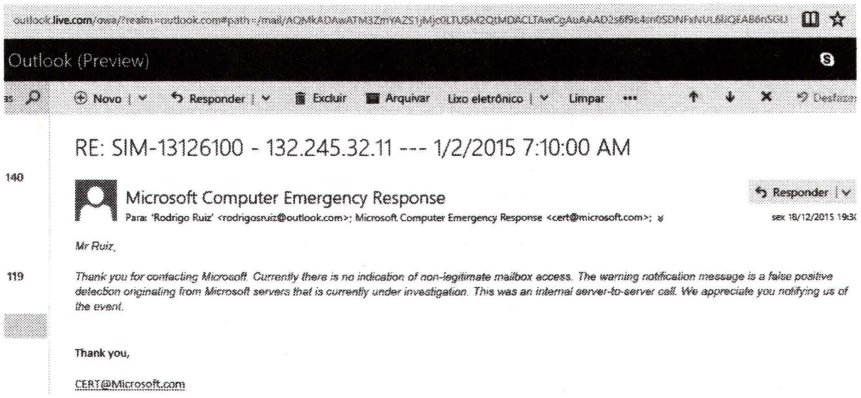
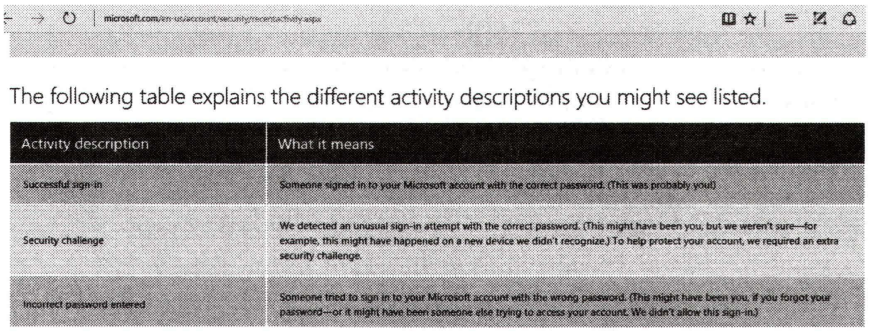

Outlook (Preview)
Novo
Responder
Excluir
Arquivar
Lixo eletrônico
Limpar
RE: SIM-13126100 - 132.245.32.11 --- 1/2/2015 7:10:00 AM
Microsoft Computer Emergency Response
Responder
Mr Ruiz,
Thank you for contacting Microsoft. Currently there is no indication of non-legitimate mailbox access. The warning notification message is a false positive detection originating from Microsoft servers that is currently under investigation. This was an internal server-to-server call. We appreciate you notifying us of the event.
Thank you,
CERT@Microsoft.com

Figure 4. Microsoft's response that the incident in question is just a false positive with regard to its own server-to-server communications: "Thank you for contacting Microsoft. Currently there is no indication of non-legitimate mailbox access. The warning notification message is a false positive detection originating from Microsoft servers that is currently under investigation. This was an internal server-to-server call. We appreciate you notifying us of the event."

This answer does not correspond to the information that Microsoft published on its site[12] about the security and privacy of Outlook (see Figures 5, 6, and 7). On the same page, Microsoft says: "When you tell us that you don't recognize an activity, it's possible that a hacker or a malicious user has gotten access to your account. To help protect your account, we'll walk you through several steps, including changing your password and reviewing and updating your security info."



The following table explains the different activity descriptions you might see listed.

Activity description	What it means
Successful sign-in	Someone signed in to your Microsoft account with the correct password. (This was probably you!)
Security challenge	We detected an unusual sign-in attempt with the correct password. (This might have been you, but we weren't sure—for example, this might have happened on a new device we didn't recognize.) To help protect your account, we required an extra security challenge.
Incorrect password entered	Someone tried to sign in to your Microsoft account with the wrong password. (This might have been you, if you forgot your password—or it might have been someone else trying to access your account. We didn't allow this sign-in.)

Figure 5. Microsoft describes on the user's page[12] the different activities relating to an Outlook access report.

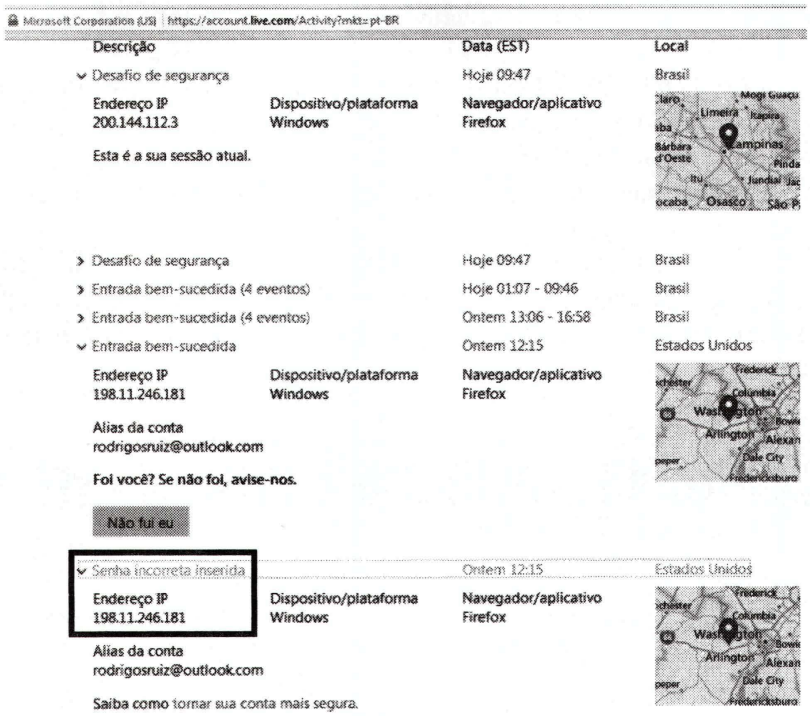


Figure 6. A wrong password was typed in by a human in Washington DC a few days before London got access to the email account. "Senha incorreta inserida" is Portuguese for "Wrong password typed."

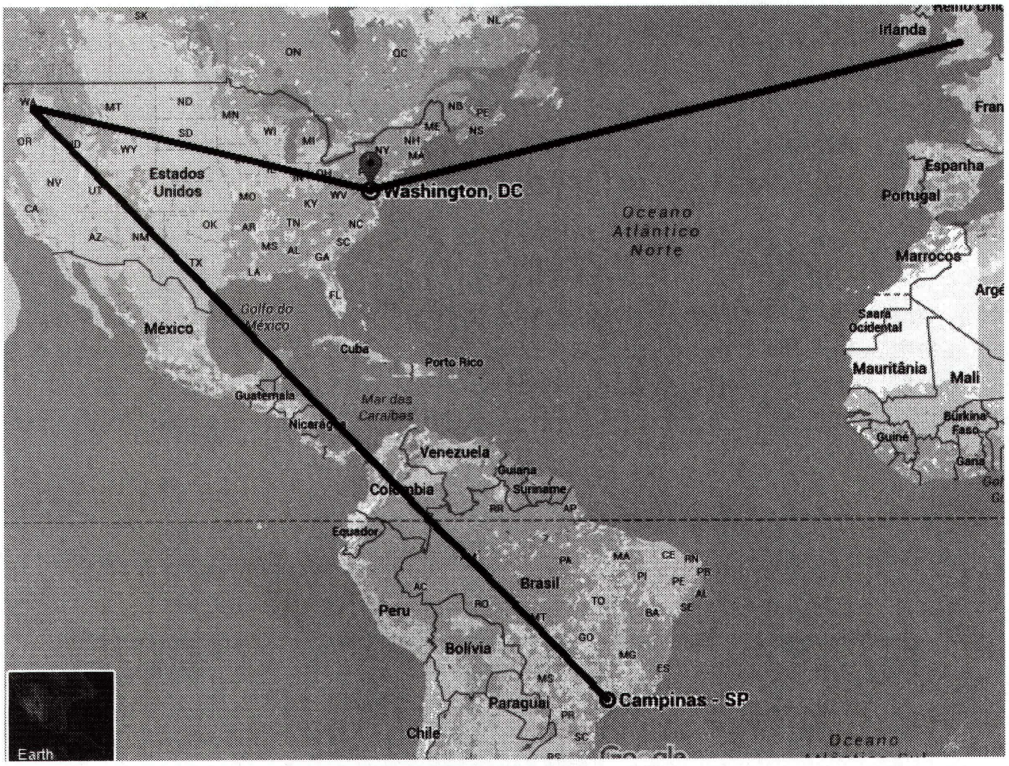


Figure 7. The way of shame, starting in Brazil, where the real user accessed their webmail and where the hacking took place in Microsoft, connecting in Washington DC, and finally arriving in London. Image from Google Maps.

More Questions Than Answers

What are the conditions that might have led to the UK becoming involved in this incident? Or was the UK government also a victim, ashamed to admit that it had been hacked? And did Micro-

soft fall prey to one of its employees? What is the impact of this type of espionage in the world on researchers and the general public? Are thousands of researchers vulnerable to the shady methods and almost unlimited resources of organized hackers? How many patents are at risk? Is the crime no longer about stealing, but simply getting caught? The *Los Angeles Times* reported in 2001 that the relationship between scientific researchers and intelligence agencies did not cool off after the Cold War as previously thought. But, while these researchers continue to fully cooperate with their intelligence masters[13], they should not forget that the same person who pays the wages of these scientists may also be reading their emails on a daily basis.

References

[1] SSL.COM; "What is SSL?;" http://info.ssl.com/article➥.aspx?id=10241

[2] NSA.GOV; National Security Agency; https://www.nsa.gov/

[3] CIA.GOV; Central Intelligence Agency; https://www.cia.gov/index.html

[4] GOVERNMENT.RU; "The Russian Goverment;" http://government.ru➥/en/department/113/

[5] MacAskill, Ewen and Dance, Gabriel; "NSA Files Decoded;" *The Guardian;* 11 November 2013; http://www.➥theguardian.com/world/inter➥active/2013/nov/01/snowden-➥nsa-files-surveillance-revel➥ations-decoded

[6] Schneier, Bruce; "Securing Medical Research: A Cybersecurity Point of View;" *Science,* Vol. 336, pp. 1527 - 1529, 22 June 2012

[7] American Association for the Advancement of Science; "The End of Privacy;" *Science,* January 2015; http://www.➥sciencemag.org/site/special/➥privacy/index.xhtml

[8] Greenwald, Glenn et al; "Microsoft Handed the NSA Access to Encrypted Messages;" *The Guardian,* 12 July 2013; https://www.theguardian.com/➥world/2013/jul/11/microsoft-➥nsa-collaboration-user-data

[9] American Registry for Internet Numbers; https://www.arin.net

[10] RIPE Network Coordination Centre; https://www.ripe.net/

[11] UK Ministry of Defense; https://➥www.gov.uk/government/organ➥isations/ministry-of-defence

[12] Microsoft; "What is the Recent activity page?;" http://www.microsoft.com/➥en-us/account/security/recent➥activity.aspx

[13] Gibbs, David N.; "Academics and Spies: The Silence That Roars;" *Los Angeles Times,* 28 January 2001; http://art➥icles.latimes.com/2001/➥jan/28/opinion/op-18012

Acknowledgment

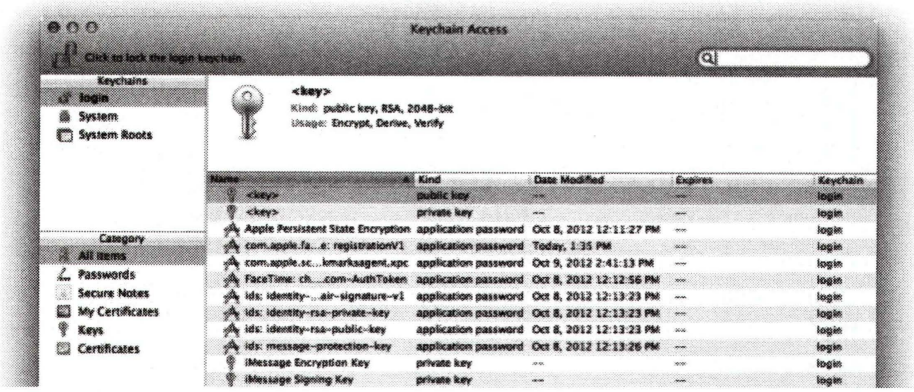
Thanks for all, *2600* team. Thanks to Kil Park and Fernando Amatte for research with us in crypto, privacy, and *Apoc@lypse*. These surveys are catching the attention of the world. Thank you for our wives who encourage us.

Biography

Rodrigo Ruiz is a researcher at Centro de Tecnologia da Informação Renato Archer, Campinas, Brazil. In addition, he is a member of the Society of Digital Information and Wireless Communications, as well as the co-author of Apoc@lypse: The End of Antivirus. *He has also authored papers about privacy and security for* Cyber Defense Magazine, Cyber Security Review, *and international conferences and journals.*

Rogério Winter is a colonel in the Brazilian Army with more than 25 years of experience in military operations and information security. He holds a master's degree in electronic engineering and computation from the Instituto Tecnológico de Aeronáutica and is a member of the Society of Digital Information and Wireless Communications. His current interests are warfare issues, cybernetics, command and control, and decision-making processes. He is also the co-author of Apoc@lypse: The End of Antivirus.

InfoSec at Its Worst, OPSEC at Its Best


Keychain Access
Click to lock the login keychain.
Keychains
login
System
System Roots
Category
All Items
Passwords
Secure Notes
My Certificates
Keys
Certificates
<key>
Kind: public key, RSA, 2048-bit
Usage: Encrypt, Derive, Verify
Name
Kind
Date Modified
Expires
Keychain
<key> public key — — login
<key> private key — — login
Apple Persistent State Encryption application password Oct 8, 2012 12:11:27 PM — login
com.apple.fa...e: registrationV1 application password Today, 1:35 PM — login
com.apple.sc...kmarksagent.xpc application password Oct 9, 2012 2:41:13 PM — login
FaceTime: ch....com-AuthToken application password Oct 8, 2012 12:12:56 PM — login
ids: identity-...air-signature-v1 application password Oct 8, 2012 12:13:23 PM — login
ids: identity-rsa-private-key application password Oct 8, 2012 12:13:23 PM — login
ids: identity-rsa-public-key application password Oct 8, 2012 12:13:23 PM — login
ids: message-protection-key application password Oct 8, 2012 12:13:26 PM — login
iMessage Encryption Key private key — — login
iMessage Signing Key private key — — login

by NerveGas Jr.

Introduction 0x0

As I write this, I am on my mother's Mac computer as she and my stepfather play *Call of Duty: Advanced Warfare* on the PS4. In order to get on the Wi-Fi for this computer, I had to ask my stepfather to unblock the computer from the Wi-Fi to write the article, which is ironic as you will see. Years ago in 2012, my mother gave me the password to her Apple account so I could update the apps I had on my iPod. Years later in the summer of 2015, that password came in handy when I needed access to her computer to contact someone and she wouldn't let me. As you may have guessed, the computer had the same password on it as her iTunes account. And it didn't stop there....

Genesis, Exodus, Revelation 0x1

As previously stated, I needed a password in order to update my apps for my iPod and, since my mother was thousands of miles away from me for a prolonged period of time, I needed her to text me the password to update, because if I didn't, I would soon be cut off from all media, and then from the whole world basically, because that is how our world is now. She texted me the password, hexxxx5Got. I used it to update the apps and for nothing else, but I remembered it because I like to remember things I might be able to use later. Eventually, my iPod got taken away, but I still remembered the password. A few years after that, we moved from one state to another and my mother moved to a different one for reasons that will remain unstated. Over the summers, I got to see her and every summer I got closer to needing her password for the computer.

One summer, the computer was locked with a password because my mother didn't want my other siblings to have access to it, and I got the short end of the stick. One evening, when my parents were downtown, I decided to have a crack at guessing the password. I guessed things my mother might have used as the password like her birthday, qwerty, and the like. After a few guesses, I had a eureka moment and guessed the password she had given to me years earlier back in 2012, hexxxx5Got. It worked, and after contacting the person I needed to, I decided to have a poke around, because why not? *Maybe* I would get caught, but maybe I wouldn't.

Mac OS X has a built-in password-saving application called Keychain Access, which was where I started. I had access to an iPad that wasn't yet connected to the Wi-Fi and, if I could only get Wi-Fi on that iPad, I wouldn't need to sneak onto the computer. It would be more efficient. So I went into Keychain Access to acquire the password. KeyChain Access by default has password protection that most people use to ensure that others can't get into it to get the passwords. In this pitiful case, the password was hexxxx5Got, which was my first guess. I got the Internet password, which surprisingly wasn't the same as the Apple account, computer, and Keychain Access. It was a combination of my mother's last name, my brother's name, and some other number. I quickly memorized that and then got out of the computer.

After finding the iPad, I turned it on. I was baffled to see that it then had a password on it - probably to keep my siblings out of that too - but I didn't worry about having the short end of the stick. The password was unsurprisingly hexxxx5Got. I entered the Wi-Fi password and was able to use the Ipad for the rest of the summer with no problem. It was easier to sneak around with and more efficient to use for contacting people and for covering my tracks.

One Year Later... 0x2

After leaving my mother's to start school, I forgot all about the technical adventure I had and lived my life without any problem, that is, until I went back for this summer. My siblings used the computer nonstop since the password was taken off and they love their Minecraft videos and make-up tutorials. Eventually, my stepfather set up the Wi-Fi (using Linksys Smart Wi-Fi Application) to block the computer from the Wi-Fi during the times when neither of my parents were home. The only way to unlock the Wi-Fi was to go into the Internet browser and login to the Linksys Smart Wi-Fi Application with an email and password. The password wasn't the problem because I knew it would be the Internet password, which I could find through Keychain Access in a minute. It was amusing that the email address was my problem because everyone always needs the password, but here that just wasn't the case. Fortunately, they were using Gmail and the Gmail address was saved in the login page.

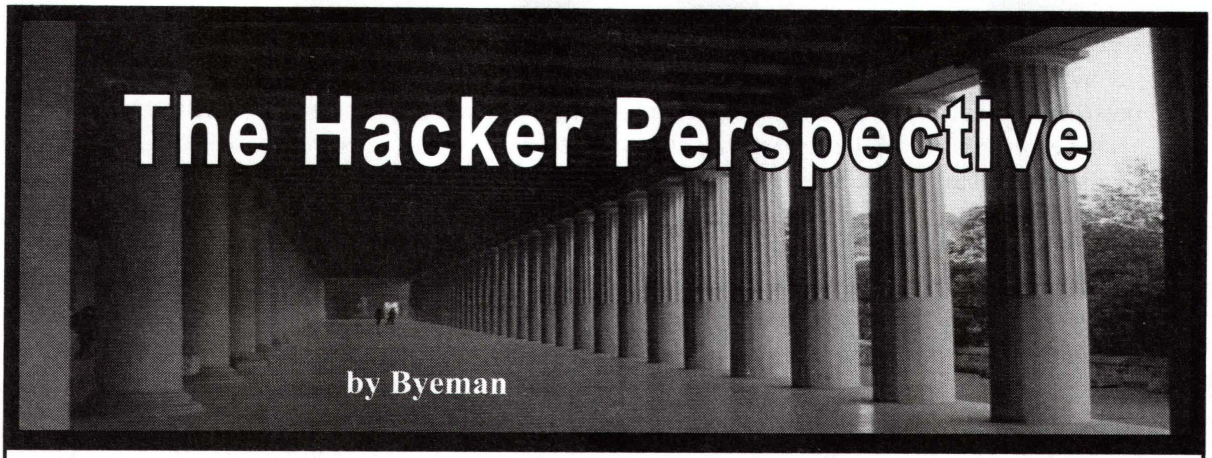
So I logged into the Linksys Smart Wi-Fi Application and changed the settings so I could go onto the computer in order to do summer homework (high school sucks). I knew that my stepfather would be able to tell that the computer was connected to the Internet by looking at the status from the app on his phone, but I was able to get the computer incognito so I wouldn't get caught. I went in, did what I had to do, and then got out and changed the settings back to its previous values to cover my tracks. To further cover myself, I deleted the history from the previous five minutes on the browser and computer. Then I poked around in Keychain Access again.

My mother needs InfoSec training bad. Her Amazon account details were in there, along with her Social Security number, LinkedIn, Facebook, Instagram, credit card information, and pretty much every other password she had ever used, at least that she had ever used on that computer. I didn't need to use any of these, except maybe the credit card information (just kidding, I'm not that rude, and those tracks are harder to cover - as if she would check). My brother has a tablet which I used for a while, but eventually the Wi-Fi was blocked so my brother couldn't use it, which was no problem for me either. Basically, I knew every password my mother and stepfather had, along with their socials. I had another idea as I was trying to crack my mother's phone password so I could amaze her by "guessing" it. A day earlier, she gave my her account login code for the PS4 so I could play it and, after asking her where she got the seemingly random four digit combination, she told me plainly "the last four digits of my Social Security number." I almost knew that she used her whole Social Security number for the password since it was nine digits long, as Social Security numbers are (I tried to get the password to the phone by shoulder surfing, but she put it in too fast for me). Surely enough, her password was, and still is, her Social Security number. I didn't look though her phone because I was already preoccupied, but maybe later!

Conclusion 0x3

Only my hacker father knows that I know my mother's and stepfather's passwords and everything else, and he won't tell, well... because he's cool. Even if he does, I'll probably be able to figure the new passwords out anyway. In the Keychain Access, there were variants of the password hexxxx5Got such as jexxxx6Got. While it's good to use variants for a little more password protection and easy memory, it can be dumb if you have a 15-year-old hacker son. I didn't use any coding or go through any partitions to get passwords - I simply used my tiny amount of knowledge about my mother's passwords and went from there to get almost all of them. I deleted my passwords from the Keychain Access so no one could snoop around *my* stuff and I covered all of my tracks. In the end, I wound up using my Mother's bad InfoSec practices for my own good InfoSec habits. I was cautious of covering my tracks the whole time in order to maintain good OPSEC. Even now while I finish this article, I'm doing that. If my stepfather or mother walk in here, I can switch to the draft email of my summer homework (again, high school sucks), and go back to this when they decide to play *Call of Duty* again, which they are still doing. Cheerio! Happy Hacking!

The Hacker Perspective



by Byeman

I work in the high tech industry. Despite my coworkers' backgrounds, they still view hackers as lazy millennials living in their parents' house not paying back their $150,000 in student loans who use their idle time to steal from those like us who sit in conference rooms all day wondering how we're going to make the next installment on our $150,000 mortgages.

I too am a hacker. I didn't always embrace the label. In fact, I often ran away from it. I've made a few trips around the sun having been around for most of the Nixon administration (if you're one of these who believes life begins at conception, I was around for the tail end of the Johnson years). Since the early 1980s, I understood the distinction between "hacker" and "criminal who uses technology to commit crimes." I was your typical self-conscious, high-strung, 13-year-old who looked down upon those comic book loving, *Dungeons & Dragons* playing, VIC-20 owners. They were the hackers, I was the normal one. Right? Thankfully, I outgrew that narrow definition and lately have been reflecting on my hacker roots. Why, you ask? I'll tell you why.

My career has taken me all over the world. I was sitting in an oyster bar in Guadalajara with some coworkers and one of them asked how I came to be so curious and knowledgeable about the world around me. Their inclination was to head to Chili's for familiar food and Coke. I insisted instead on us visiting that hole in the wall a few blocks away with damned good food and real tequila (not the crap found in most frat houses back home). I don't speak Spanish, but I don't care. I plow through my mangled español with gusto. It occurred to me amongst other talents that I'm also a language and travel hacker. An unfamiliar language and marginally different culture isn't something to avoid, but to crack apart, understand, and misuse until I finally master it. I really think the hacking skills I began to develop with I was five years old continue to serve me forty years later.

The day I turned five was a momentous event. Actually, it probably wasn't, but I was to start kindergarten shortly after and my grandparents saw fit to present me with a clock radio. Because, you know, it's never too early to get your firstborn grandson indoctrinated to the whole 9 to 5 routine. My birthday candles hadn't been lit before I took a screwdriver to it to figure out how it worked. How did this plastic box know to flip the mechanical number to the next value every minute? How did it magically go from 59 back to 00 and not 60? I saw a litany of gears and moving parts and figured out which ones controlled the minutes and which the hours. I also got introduced to what 120 VAC feels like. That evening I was still geeking out, this time with the radio. It was AM only and I started hearing stations that weren't there earlier in the day from cities I had never heard of. I found my dad's road atlas and discovered just how far away the likes of KRLD, KOMO, WSM, and WLS were from my house. This was my gateway drug. I started learning about electronics, I read how nighttime radio propagation works, and I became more methodical in my exploration. I figured out there was 10 kHz spacing. I would actively seek less active spots on the dial to see what I could pull out of the static. Besides igniting my curiosity, I believe this taught me at an early age to ask questions, go to the library, and learn, learn, learn.

My parents were generally supportive, but I did bump up against the parental proxy server which made me only more curious and more determined. I had come across my mom's pregnancy books and she didn't think an elementary aged boy should be reading about ovulation cycles or how a placenta works. This is a rather graphic example, but just goes to show to what lengths the system will go to so it can "protect"

children from "harmful" knowledge. And I proved once again how fruitless such efforts are. Had my mom shrugged it off, I probably would have tossed the books back in the box. Instead, I became more determined than ever to learn.

It was after a move from the Deep South to the banks of the Ohio River where I found the previously unpacked box of my mom's books. I also found our "rabbit ears" TV antenna. We were in rural Appalachia where cable television was a necessity. I connected the antenna to an old telephone and could hear the Voice of America coming from the speaker. My parents were stunned and compared me to the professor on *Gilligan's Island*. I now know I didn't do anything spectacular. In reality, we weren't too far from VOA's Ohio transmitter site and any length of wire and speaker could pull in their signal. This lesson came home over ten years later while in college when I bought some new stereo speakers, only to learn when I moved them to opposite sides of the room, creating an antenna with the speaker wire, the local 50 kW flamethrower would bleed through.

Speaking of cable television and parental firewalls, we didn't have a cable box. Instead, various Ohio, Kentucky, and West Virginia TV stations were mapped to channels 2 through 13. This being the 1970s, we didn't have nice things like digital tuners. I noticed a flicker when I switched between channels 6 and 7. This intrigued me. I did not see that flicker between any other channels. I fiddled with the knob until it was halfway between 6 and 7 and I had a commercial-free movie. It was titled *Eat My Dust!* and starred Ron Howard whom I knew to be Richie Cunningham from *Happy Days*. There was a scene where a woman, who might have been naked, got into the shower with "Richie." This brought down the roof, my parents demanding to know what I was watching. I explained what I had done and I got a lecture about watching "inappropriate" shows and "stealing" HBO. Although it didn't stop them from watching *Orca* later that evening or asking me for help getting the knob just right between those two channels.

Hacking doesn't always involve technology. Despite the stereotype of the straight A nerd, I liked sports. I just wasn't very good. The one sport I excelled at was running, so I joined my high school's cross country and track teams. By this point, I had a Tandy 1000 computer. I wrote a Pascal program and used it to log my times from races and I noticed quite a bit of variation from week to week. "Why?" my inner hacker asked. I started logging my splits, my training during the week, what I ate, how much I slept, etc. In my case, it was food that most affected my times. Since my meets were in the early evening, I left right from school on a bus and went to the venue. My mom would buy me canned food that I could eat there. This opened a plethora of sophomoric male jokes, but when I ate chili, my legs (or other parts) seemed to propel my body to the finish line the fastest. So that became my pre-race meal and it's what got me on the varsity team.

Even before my running days, I had "hacked" our county's bus system. I'm using the term "hacked" here loosely. I never made the buses run faster or cracked their fare system. We had since moved to Florida by this point and, as with most Sunbelt cities in the 1980s, it was car-centric. Even the state of Florida wasn't insane enough to license 12-year-olds to drive cars. Where I couldn't go on my bicycle, I was able to ride the bus. For a mere 25 cents, I could get anywhere in the county, which happened to be slightly larger than Rhode Island. To a preteen boy who really needed to get out and explore his space, figuring out the bus system was a godsend. I would ride to the mall to buy radio magazines (*2600* didn't exist yet). I'd go to the airport to plane watch. I'd hang out downtown and visit cool shops we didn't have out in the suburbs. I developed a feel for college campuses by hanging out at USF. I was very tall for my age, well over six feet tall, so I passed as another baby-faced freshman. This gave me access to their library, student center, and bookstore.

Buses? Sure, they're boring. But it was my hacker mindset that sent me down that path. When I did eventually start driving, I already knew my city like the back of my hand. I was shocked that many of my friends didn't have life skills I took for granted like getting from point A to point B. Buying groceries. Talking to adults, asking questions, getting directions. Hacking is what separated me from being a lonely, homebound, angst-ridden, latchkey teen who would starting making bad decisions with respect to drugs and alcohol out of sheer boredom.

Those quarter bus rides started to add up, so I mowed lawns to fund my habit. I used to joke that a kid could make a lot of money in Florida cutting grass or selling it. I wanted to stay legal,

so I used my dad's lawnmower. Like with all tools, the mower didn't always work when I needed it to work. I learned the hard way that taking the mower in for repair could eat up a week's pay and left me unable to mow lawns. So I disassembled the mower, engine and all, and figured out how it worked as I put it back together. If I could only have read women like I read power tools, I would have had it made. I could hear every unusual ping, feel every unexpected vibration, and knew what I had to do to go fix it.

<TMI>As an aside, I wasn't completely inept with women. They just happened to all be much older than me. Most of my teachers were women. From my years of acquiring "carnal" knowledge, I knew their moods would change in a predictable and periodic manner. I was at the time about 6' 3" and athletically built, and I was able to sweet talk certain teachers during certain weeks when my assignments weren't quite actually all the way done (or even started). I've told this to some women and all of them have told me I'm full of shit. But it did seem to work much of the time and taught me valuable lessons about social engineering.</TMI>

But my life as a hacker hasn't always been fun and games, nor has it always worked to my advantage. While in college, I worked for a major telephone company. Email was still an odd beast and many folks at work still relied on intra-office mail, paying someone to hand carry typewritten pieces of paper on company letterhead from one floor to another, only to have it read and thrown out in less than 20 seconds. I was already familiar with username@domain.tld and, when back at school, I started emailing my coworkers who actually used email. Overnight I was that college kid who hacked into their computers. Some of the saner heads prevailed after I demonstrated their email system wasn't internal, but rather connected to a global network. Soon I was the go to guy when someone needed to know how to email an old friend living in Italy. It's a good thing I never took a copy of *2600* to work with me.

After graduating from college, I started my first "real" job. Throughout college, I used UNIX almost exclusively and it was a shock to be thrown onto something as archaic as Windows 3.1. I found a sys admin and appealed to his ego by praising all that is UNIX and getting an account on "his" system. It took me no time at all to find the /etc/hosts file, giving me the names of various servers to go explore. Most allowed anonymous FTP access, even from outside the company's network. I found an unencrypted text file containing the name, address, date of birth, Social Security number, employee number, and rate of pay of every employee. I reported this and was immediately thanked and given a corner office with a window. Oh, who am I kidding? I was accused of "hacking" and told I would lose my UNIX account. My account didn't go away until that machine was decommissioned years later. And as for the file of employee records, it continued to be available and was regularly updated. Nothing else happened to me, but this shows once again (as discussed between these covers every single issue) that it's those who expose the truth who find themselves on the receiving end of management's anger, not the incompetents who made the mistake in the first place.

No, I never accessed Pentagon computers. I never changed grades or stole credit card numbers. My hacking was far more mundane, but when I look back at it I realize it has made my life much more interesting and has made me a better problem solver and, best of all, a better person.

If you're reading this and you're young enough to be my daughter or my son, don't wait for someone to give you permission to learn. Today, most of you carry the world's knowledge in a palm-sized piece of metal, glass, and silicon. Enter the make and model of your microwave oven so you can learn how it works. Find a way to get to a local college. See if you can sit in on classes. Watch their website for any seminars or guest lecturers who might impart knowledge you know you want. Start talking to adults. I don't mean the ones who drive windowless vans with "free candy" hand-painted on the side, but your parents' friends, neighbors, teachers. While we might not look the part, many of us are hackers at heart and would enjoy passing on our knowledge.

The author is still a reluctant hacker working in the manufacturing industry and still continuing to travel the world. When he's not working his day job, you'll likely find him at home reading, hiking Austin's trails, or catching Pokemon with his son.

HACKER PERSPECTIVE submissions are closed for now.
We will open them again in the future so have your submission ready!

<?xml version='1.0' encoding='UTF-8'?><article><title>Can Security Be Built into Pure Data?</title>

by Wyatt Lee
worlduniversity@mail.com

This is a question that might not make much sense when you first read it. In fact, it's probably gibberish. For this reason, this article is not going to follow the traditional problem, solution, conclusion format. Instead of starting with the problem and giving a solution, I'm going to start with a question, explain how why the question makes sense, and end with an interesting challenge to every ethical hacker.

Imagine you're a developer commissioned to build a web app of some kind. No matter what architecture you choose or what that app does, it is probably going to involve parsing some XML and rendering it in a human readable form. Other alternatives, of course, are using relational databases to store data, but this is a field in itself and much is known about best practices for interacting with these types of data stores, like avoiding SQL injections, so we will restrict ourselves to considering the following:

(1) Some web application which may be, for example, a Node.JS app that runs completely in the backend or a JavaScript front-end app that writes data to the browser's cache or your hard drive.

(2) User data is stored as some kind of XML on disk or in the browser's cache (less secure).

The first example could be a web browser which reads in HTML, CSS, and JavaScript and renders it in the browser's GUI. This architecture, which has been used since the 90s, presupposes that security should be the responsibility of the browser as a second line of defense after the router and any packet filtering firewall or intrusion detection system you have installed.

The question I would like to put forth is, is this necessary? Why not just have a secure XML document so that additional security is built into the data itself?

Why would this be beneficial? Because it would greatly reduce the need for browsers to be secure. Now, assuming you're with me so far, how do we do such a thing?

What I am proposing is a secure XML standard for an additional layer of security between the browser (or even a mobile app or apps running in the cloud or fog) and possibly malicious packets of data (whether they can be decoded to XML or not). An extra layer of security for virtually no overhead is always a good idea.

Consider the following piece of XML like code:

```
<data format = "JSON" ,
➥      key = "Your Key Here">
  <code>
  /* JSON file here */
  </code>
</data>
```

A simple parser could easily be written that takes any document of this form sent over the web and have a separate validation server parse it in a secure way (this would be more secure than most general purpose parsers that are more complex and thus may have bugs).

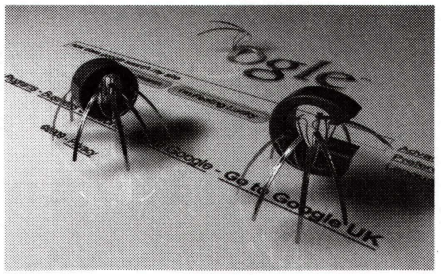
Such a parser could be formally verified quite easily. The string between <code> and </code> would ideally be separated physically in memory, preferably on a cluster where nodes are physically separated in space.

A map reduce validation algorithm can then be used to decide if the data is suspicious or not, minimizing the risk of buffer overflow attacks because each worker node's memory is physically isolated and would receive a random portion of the string.

Once this validation phase is over, the data could be verified with the key, which is a checksum of the validated data.

If anybody is interested in meeting and turning this into a cryptographic protocol for very sensitive applications on the web such as apps running in the cloud, or wants to propose some open standards for a secure XML for crypto applications, send me an email.

mcquery.js - A Web Scraper for Disc Golf Players



by Brenden Hyde

Disclaimer: I am not a corporate shill for Innova or any other company; I'm just an obsessive fanboy.

Introduction

Each summer my girlfriend and I seem to have a new obsession. This year it's disc golf. In addition to playing every day, we also watch the professionals play tournaments on YouTube. The highest-rated player in the world right now is Paul McBeth who is sponsored by Innova. As part of his sponsorship, they make a special golf disc for him called the "McPro Roc3." It's a highly sought-after disc because of its limited releases, and it always sells out extremely quickly. I had tried and failed several times to manually keep tabs on their sales, but I was always too late to order one. To add insult to injury, there were near-constant brag posts on Reddit by those who were lucky enough to snag one. They sold on eBay for around double the price, but I didn't want one badly enough to pay the mark-up. That's why I decided to write a simple web scraper to keep tabs on the site for me.

Planning

I am no developer by trade, but I had dabbled in NodeJS through a YouTube series called "The Net Ninja," so I decided to use that. With the language chosen, I started to plan out what I wanted the app to do, which on paper was only two things:

1. Periodically check the McPro Roc3 sales page for available inventory.
2. If there was inventory, send me a text message with a link to the page.

Preparation

I used Debian for my Linux distribution, but any distro should work.

First, I downloaded NodeJS from `nodejs.org`, which includes Node itself as well as Node Package Manager (npm). Installing them is beyond the scope of this article, but there are plenty of tutorials to get up and running.

In addition to node and npm, I used three external NodeJS modules called "request", "cheerio", and "twilio". The request module let me make "HTTP GET" requests to Innova's website to download the product page, and the cheerio module let me parse through the HTML to find the section that could tell me whether or not they had inventory. Twilio is a paid SMS gateway service that requires an account, and it allowed my scraper to text me when my precious disc became available. To install the external modules, I ran these commands:

```
npm init -f
npm install twilio -save
npm install cheerio -save
npm install request -save
```

The first command created my package.json file (more on that in a minute). The "-save" option in the commands adds them to the "dependencies" section of the "package.json" file. This in turn allows others to more easily run your app by taking care of all the dependencies. To install all dependencies from someone else's "package.json" file, just change directories to the location of the json file and run:

```
npm install
```

Beyond installing those modules, there was some actual programming involved, but describing that here would be boring. I have added some comments in the code section that hopefully explain my rationale.

Outcome

I programmed the mcquery.js scraper over the course of four to five hours at work (please don't tell my boss), and when I got home, I excitedly explained the concept to my girlfriend and initialized the program for a demo run with this command:

```
node mcquery.js
```

It was written to check the inventory status every 30 seconds and to spit out the result to my command line. It was a neverending, scrolling terminal that looked eerily like an homage to *The Shining*:

```
availability out-of-stock
availability out-of-stock
availability out-of-stock
availability out-of-stock
availability out-of-stock
availability out-of-stock
availability out-of-stock
```

I expected to see a lot more where that came from since there were often month-long gaps between releases, so I left the program running and walked away.

About 20 minutes later I felt the buzz of a text message in my pocket, and when I checked my text messages, I saw those glorious words:

```
McPro Roc3s are in stock again! (hyperlink to site)
```

At first I assumed my app had malfunctioned, since I had received dozens of messages like that throughout my testing that day. I went to the site, and sure enough my scraper had done its job! I unashamedly bought one in every color and laughed an evil victory laugh. Obsessive? Yes. Unnecessary? Probably (considering their Twitter feed has the same information). But who has the disc now? *Who. Has. The. Disc. Now?!*

Give Me the Codez

```
//BEGINNING OF mcquery.js

var request = require('request');
var cheerio = require('cheerio');
var twilio = require('twilio');
var accountSid = 'xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx';
➥      //replace w/ real SID
var authToken = 'xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx';
➥      //replace w/ real
authToken
var client = new twilio.RestClient(accountSid, authToken);
var requrl = 'http://proshop.innovadiscs.com/mcpro-roc3.html'
var textStr = "McPro Roc3s are in stock again!\n" + requrl;
var status = '';

function rocquest(err, resp, body){          //makes HTTP GET request
➥      to Innova
   if(!err && resp.statusCode == 200){
var $ = cheerio.load(body);
$("p[class~='availability']").each(function(){
  status = this.attribs.class;
  console.log(status);
});
   }}

var sendAlert = function(){ //Sends text message when discs in stock
   client.messages.create({
body: textStr,
```

```
to: '+19705552600,  // Text this number (change as needed)
from: '+19704202600' // From a valid Twilio number
   }, function(err, message) {
if(err) {
  console.error(err.message);
} else {
  console.log(message.sid);
}
   });
};

var mcquery = function(){ //check status and send text if available
   request(requrl, rocquest);
   if(status.includes('availability in-stock')){
clearInterval(loop);
sendAlert();
   }
};

var loop = setInterval(mcquery, 30000);     //starts the program by
➥      invoking a loop

//END OF mcquery.js

//BEGINNING OF package.json (do not include this line or the end
➥      line)

{
 "name": "mcquery.js",
 "version": "1.0.0",
 "description": "Query Innova's Pro Shop for new McPro Roc3 discs",
 "main": "mcquery.js",
 "scripts": {
   "test": "echo \"Error: no test specified\" && exit 1"
 },
 "author": "Brenden Hyde",
 "license": "ISC",
 "dependencies": {
   "cheerio": "^0.20.0",
   "request": "^2.73.0",
   "twilio": "^2.9.1"
 }
}

//END OF package.json

//BEGINNING OF README.txt

mcquery.js Version 0.1.0
------------------------
DESCRIPTION

mcquery.js is used to check the stock status of McPro Roc3 discs
➥      in the Innova Pro Shop.

USAGE

1.) Install nodejs from nodejs.org and link the node and
npm bin files to your $PATH environment variable.
2.) cd to the directory where mcquery.js is located.
```

```
3.) Type "npm install" to install program
dependencies (twilio, request, cheerio).
4.) Type "node mcquery.js" to run the program. This will spit out
the availability status to the console every 30 seconds by default
- this default can be changed in the loop() function by removing the
"3000" and replacing with the appropriate number of milliseconds.
Once the availability changes to "availability in-stock," a text is
sent to the phone number referenced in the sendAlert() function.

NOTES

1.) The mcquery function checks Innova's Pro Shop for the
status of the McPro Roc3. It uses the external "request"
module with a URL and callback function as parameters.
2.) rocquest is the callback function for mcquery (2nd
parameter). This function uses the external "cheerio" module
to do JQuery HTML DOM parsing to find the paragraph with
the availability status (in-stock or out-of-stock).
3.) The status variable is a global variable that is
modified by rocquest and is a string that either says
"availability in-stock" or "availability out-of-stock".
4.) The status is set each time mcquery() is called. This
is done periodically because the status will change at
some point from "out-of-stock" to "in-stock". Therefore,
mcquery needs to be called repeatedly in a loop.
5.) setInterval is the function that will call mcquery every
n milliseconds. n is set to 30000 milliseconds (30 seconds)
by default. It will need to be cleared when the status no
longer requires updating (i.e., the disc is in stock).
6.) loop will be the function that acts as a wrapper for
setInterval calling mcquery. As the name implies, it is a
loop which will run until it has served its purpose.
7.) clearInterval is the function that will stop
setInterval from repeatedly running mcquery. It takes
only one parameter, in this case "loop".
8.) sendAlert is the function which will send a text message to me
(you?) once the status is set to "in-stock". It only needs to be
called once, right after the loop is stopped with clearInterval.

//END OF README.txt
```

Acknowledgment

Smitha Milli's YouTube video on web scraping with Cheerio and Request was a large chunk of my program. It's available at `https://www.youtube.com/watch?v=LJHpm0J688Y`.

ATTENTION WRITERS

You now get more when you have an article published in *2600*

For each article printed, you'll receive:

One year of *2600* (subscription, back issues, paper/digital)

AND

One of our *2600* hacker t-shirts

(that "AND" used to be an "OR")

CROSSFIRE

General Inquiries

Dear *2600*:

First of all, thank you guys for publishing me, now twice! I can't believe it was started by someone I know who spoke at one of the HOPE conferences and brought back a couple of issues of *2600* for me to read. I spent hours reading them over and over again, loving everything. I started to buy issues whenever we went to the Books-A-Million store 90 minutes away. Then I figured out that I could get free subscriptions by getting articles published. So I wrote one, sent it in, and a couple of months later saw it in the magazine. It was a simple back door, but I still got the free sub. If I had the money, I would buy them, and I will be supporting you guys through buying each issue and not a lifetime so that you keep getting money from me. Thanks for being awesome.

Anyway, the same person that started me with *2600* is a great, genius programmer and hacker. I've started to learn some Bash scripting, but when I don't know something, all the help I ever get is RTFM, which is common, but ridiculous for someone like me who only has two hours a day on the computer, counting assignments. If I could stay up all night and RTFM, I would, but I can't. Do you guys know of a hacker forum that is kid-friendly in any way? I would buy books, but again, I have no money for the Friggin Manuals, and it takes forever to learn from looking through online forums.

Two more questions: I am trying to download all of the PDFs for a site, but don't want to visit each page and manually do it. It is also a login site, so running a web crawler isn't working. Is there a way I can write either a Bash or maybe Python script to download and parse everything? And if you don't know, then how can I go about decoding the site to find all of the PDF links since the index is nearly impossible to find?

Please don't tell me to RTFM. I know how tempting it is, but you guys know the fine line between good sarcasm and jackass sarcasm. I will laugh, though, if you decide to say it. Then I'll cry. Then I'll RTFM for the last F'n time. Hack the planet!

Anonymous Teen

We applaud your spirit and hope you don't get discouraged with the impatience of others. It's easy to transfer people over to manuals and websites because there's no work whatsoever involved in that and there's also no risk of their own knowledge gaps being exposed. That said, manuals shouldn't be dismissed out of hand, but they can't be your only source of info. (And many times you can find them online free of charge.) Far more important is the ability to experiment. If you want to learn Bash scripting, having a machine or environment where you can try anything to see what happens is an invaluable resource. Not being afraid to break something is key. While online forums can contain helpful information, many times they devolve into tangents and misinformation. But precise searching can often lead you to someone who has experienced the exact same problem you have. The key is to be able to describe it accurately enough so that your search results prove helpful. Your age shouldn't be an issue - if it is, that's not the right place to get answers or help. Another valuable resource is personal interaction. This is why we have monthly meetings everywhere. While there are no guarantees, there is at least the chance of meeting people who understand what you're trying to do and who will respect your attempts and perhaps help theorize on what to do next. We don't know your geographical location, but it's nearly always possible to connect with an interesting group without too long a journey. Hackerspaces are another outlet for info and experimentation. It's entirely possible there's one within reach.

Regarding your quest to download a bunch of PDFs, this seems entirely doable with a utility like wget or some basic scripting. You can use Google to search that particular website for PDFs. Just go to their "advanced search" page. You might also check to see if the site has an ftp server, which might allow you to grab a bunch of files with the mget command. When you figure it out, we hope you write an article about it. Good luck.

Dear *2600*:

I recently authored a report on cybercrime. Would *2600* be interested in an article submission featuring some highlights from the report?

Steve

If you believe it would be of interest to our readers, then by all means write something up with them in mind. We're not interested in material that's self-promotional or overly corporate, but rather material that is provocative and makes some new points. In this environment, that shouldn't be too difficult.

Dear *2600*:

I'm nearing the final stages of authoring a paper and am looking for publishers that might be interested in using it. The paper itself is 23 pages. Would

this be too lengthy to be accepted by *2600*, or when it's complete should I submit it for review?

andrew

We always want to see what people write, but 23 pages is definitely a bit much. However, if the material is filled with revelations and interesting stuff, we wouldn't rule out printing it in several parts. Papers are often different than articles in tone, however, which can work against them when being considered here. A solution would be to apply some cosmetic changes that would make it more palatable for our audience. Plunging into the heart of the material sooner, having less of an academic tone, writing from the hacker perspective are all tips that can help make it a suitable length and style that would resonate with the people who read our pages.

Dear *2600*:

Sir,

Do you provide hacking tutorials?

Thank you.

hardik hardik

We appreciate the politeness, but that's not what we do. You learn hacking by doing and we can help supplement that with the various articles we print. And there's no "Sir" here.

Dear *2600*:

Hey, can someone there help me with a couple of publishing questions? I'm writing a biography and want to see if anyone can give me advice for the statute of limitations on certain criminal offenses I've never been charged with. Most of it was over 15 years ago. I think the federal is five. I was a little concerned with how the Patriot Act affects the statute on some silly stuff people used to get away with.

C

Wow, OK. We are really not the right people to ask for definitive answers on this. Legal experts definitely would know, although invariably they will likely tell you not to write about this in the first place. The safest thing for you regardless is to leave all names and identifiable information out of the piece. If it's really interesting, it won't need them anyway.

Dear *2600*:

Hi, this may be a dumb question, but it seems like I usually find *2600* on the newsstand at Barnes and Noble before I see that the website is updated. For instance, I just picked up the Autumn 2016 copy, but the website still showed the Summer 2016 issue as being on the stands. Do you purposefully wait to update the website until you think the magazine has made it to news outlets/bookstores all across the country or something? I appreciate the fact that you offer *2600* in multiple formats, but I will always read the print version.

Bill K

You're very observant - that's exactly what we do. In the past, we'd tell people the new issue was available when it actually hadn't yet made it to the bulk of stores. While we're not accepting responsibility for any of the ensuing riots that may or may not have taken place in those bookstores, we do believe people are happier when what's on our website is a fair representation of what's actually true in the real world. And if you find a new issue before we announce it, consider it a pleasant surprise.

Dear *2600*:

I wasn't sure what email address to use regarding a question I have about an article I have read in one of the issues (either 33:2 or 33:3). I went to the *2600* website and searched all over the site for a contact section, and looked through my *2600 Magazine* for a contact section, but could not find one. So I am using the contact email address found in the back of the *2600 Magazine*. I bought both of these *2600 Magazines* (33:2 and 33:3). Well, I should rephrase that. I am subscribed to the physical copy of *2600*, and I had the listed *2600 Magazines* with me while I was admitted to the hospital for just over a week. I don't know which magazine, or article in the magazine, I was reading, but I made myself a note to look up something when I got released and sent home. In my quick note to myself, I only wrote the two words "magic tree." Now that I am home, I don't remember what article that was from, and what it was regarding. I'm pretty sure it was the name of an application, but when I Google that, nothing comes up with what I would expect. I have started to go through some of the articles that I know I was reading, but could not find anything with the words "magic tree." I was hoping maybe you could help me with what article I might have been reading. I only had those two magazines with me. If I had the digital copies, it would obviously be easier to search through and find out which article I was reading. So I hope you can help me out, or pass this request on to someone who might be able to help me out. Your help would be much appreciated.

Steve W.

You certainly know how to make a challenging exercise for yourself. As it happens, all we were able to find was a penetration tester with that name from a few years ago. We made no mention of it in the issues you cited. We suggest carrying a pen so you can mark articles of interest if this ever happens again or, failing that, just fold the pages where it appears.

Dear *2600*:

In the Summer 2016 issue, you published an article by fooCount1 entitled "Free Windows." The article was great and I appreciate your work toward educating those of us who appreciate knowledge. In light of that, the AutoKMS app referenced in the document pointed to a newsnet.nl site that did *not* have the tool available for download.

Is there any way you can ask him where the tool may be acquired cleanly? A URL linking to the app would be sufficient.

Thanks in advance?

db

Consider this our asking.

Dear *2600*:

I rooted my pinball game (http://lachniet.com/pinball) - it made it to Slashdot recently.

Some people want more info on how to do it. Same as rooting any Linux OS really. It's pretty simple. The article would cover DDing a drive, converting DD to VMDK, and booting it in VirtualBox. Using single-user boot mode to add a root account. Enabling networking, ssh, etc.

Converting back, making portable binaries on a dev system and transferring, fiddling with the pinball game - CGI binaries to display on screen, streaming display to twitch.

Upside: good info for people that don't know these old tricks, applicable to more than just that one platform.

Downside: It might be a little long to write up for an article. I don't know. I haven't written it.

Mark

Well, we hope you do. While getting online attention is great, it has a completely different dynamic than the printed word, which people continue to go back to for decades (and probably centuries when we reach that stage). It's not an either/or - you can take advantage of both methods and reach all kinds of different people.

Dear *2600*:

When you say "use the highest quality settings on your camera" for payphone and back cover submissions, what does that mean, exactly? What's the lowest resolution photo you've accepted?

lol-md4

While we've been able to perform some remarkable image saving tricks, it's generally best not to use the kind of low resolution found in many camera phones. Megapixels don't always correlate to good quality. Software and image sensors play a big part, as does simply knowing how to take a decent photo. A good photographer will be able to pull it off usually, but for the rest of us, using an actual camera (such as a DSLR) with the highest resolution settings is the best bet. But if it comes down to either using what you have or not taking the picture, always take the shot and send it in. Our address is payphones@2600.com for payphone submissions and articles@2600.com for back cover photos.

Dear *2600*:

Hi all, lifetime subscriber, and have called in a few times. The Eleventh HOPE was a great time, and good job on the hotel rates.

I'm currently binge watching *Mr. Robot* and in Season 1, Episode 7 at 10m51s, the main character Elliot says: *"I remember when I was a kid I got into web design by ripping off sites I liked. All you had to do was view source on your browser."* And they show him accessing www.2600.com in a Netscape browser with things like the "Free Kevin" lockdown clock at 3 years, 4 months, 9 days, 41 minutes.

Just wondering if *Mr. Robot* ever asked, or was given permission, to use 2600.com on the show. (Or more importantly if you are owed any royalties.)

It was funny to see it, and I can't have been the first to notice it. Just thought I'd ask.

Keep up the good work.

TimInCT

Thanks for your concern and for being so remarkably precise in your observations. Yes, everything was done through the proper channels. We don't get royalties for such things - just knowing our site was one of Elliot's favorites when he was a kid was payment enough. We were quite surprised they managed to reproduce something from nearly 20 years ago with such accuracy. Incidentally, we don't believe anyone should have to ask permission to use our stuff as props. We know not everyone shares that view, but you will never catch us going after someone for not getting our OK, even if it's for a production we detest. Art should be free to express itself without lawyers.

Dear *2600*:

I understand you have a policy regarding the republishing of articles that have appeared elsewhere. I was wondering if you would be interested in making an exception in this case as it would appeal to your readers without a doubt.

Here is a link to the article. If you do decide to run it, I can send the .doc file over or whatever format you prefer. Regardless on whether you run it, keep up the good work!

Mike

The entire point of that policy is to give our readers new material. No matter how popular the piece might be, if it's already been published, we're doing them a disservice. We're not unreasonable, though. If you published it to a handful of people, that's obviously not the same thing as having it on a popular forum or website where scores have already seen it. In the end, you can always rewrite it with our audience in mind if you believe the material is still fresh. But we don't accept articles as links - you need to actually send the article to us.

Contributions

Dear *2600*:

Lopez Island, Washington - seen at the Odlin County campground. Phone lit up but no dial tone.

Tad

Fascinating, but those words were all you sent us. We suspect you intended to send along a payphone photo too. People, please doublecheck that you've actually attached your picture when writing to us. You would be amazed at how often this happens.

Dear *2600*:

I saw this one in Lindau, Germany. Touch sensitive glass with normal computer monitor located behind glass. The phone was mounted in the win-

dow of a tourist office. It allows you to call the main tourist office if the local office is closed. I think it also provides information for tourists, but only if you speak the German language needed to operate it. Without German, I could not understand how to call anyone. Great for tourists!

Here seems to be a link to the manufacturer website: http://www.tis-touristik.de/unsere-produkte/webtis-informations-systeme

Daniel

Didn't we say you'd be amazed? This was the very next submission! It seemed a shame to waste all of that exposition. Perhaps we can start a new section of pictureless payphone descriptions which would be an exercise for our readers' imaginations?

Dear *2600*:

Can you tell me, has *2600* ever in the past published any information regarding topics related to remote neural monitoring? I would be interested to know. I would also be interested to know whether or not you guys may be interested in some kind of article from someone who has been a victim for roughly five years. Try to take me seriously here, as I do realize how many people scorn at the thought of such an issue being portrayed as a reality. If you are incapable of doing so, I am obviously reaching out to the wrong people.

I feel that I have far more realistic details than many of the people who have come forward, especially those who have used mediums such as YouTube, and many of those involved in the now defunct organization FFCHS (Freedom From Covert Harassment and Surveillance). I think, however, that many genuine victims and actual experts on the subject could agree with most of what I have to say.

If you may be interested, we can go over details as to what would be an acceptable format, if such a thing would be required. I am fairly decent at writing, and I am capable of relating and expressing things as scientifically as possible, given the (basically) theoretical nature of the issue in focus, minus that which can be limited to personal experience alone.

This is an extremely important issue which needs more backing from those who have the minds to understand such things, things beyond the generic sense of paranoia that seems to be pushing so many people out there into spreading the information that they are. This goes well beyond anything regarding cyber security, though aspects of cyber security (which is lower-level security in comparison) are involved.

S

We haven't published anything comprehensive on this subject. As with most things, presentation is extremely important, and what you've outlined seems completely rational and well thought out. The concept of remote neural monitoring is fascinating and quite believable, even though many discount it as "pseudo science." Even if we believe it to be impossible, on a theoretical level, this is something those in power most definitely would want to be able to develop. We get an incredible amount of mail from people convinced their every move is being monitored and controlled, and while a good amount of these accounts may be true, they often lose believability in the telling. Perhaps this is because of the tone of desperation that can so often accompany these tales. We frequently side with the person in a film or TV show who's trying to convince everyone that they're not crazy despite the evidence and fantastic odds. In real life, this is harder to do unfortunately. Your article could do a world of good in addressing such things. Please make it as detailed as possible. We prefer ASCII format but can generally read anything.

Dear *2600*:

I know you invite article submissions, but would it be possible to accept a piece of poetry?

Thank you!

Hack the Planet
by Gregory Porter

As The Mentor once said
the electron and the switch
Is the world in which we tread

The beauty of the baud
where curiosity and intelligence
are what we applaud

Curiosity and no more.
That is my crime;
I merely opened an unlocked door.

You may stop the individual with a targeted strike,
but you can't stop us all,
because we're all alike.

Dear *2600*:

About two months ago, you notified me that my article would be published. I was trying to find out if a publication date has yet been set?

C

As we're quarterly, there are three months between issues, so this isn't at all unusual. As it can take a couple of issues for your article to show up, even more months can pass. That's why it's important that your piece not be something that only sparks interest for a short time and then is forgotten. The written word in printed form takes longer to show up, but it also sticks around for a very long time. That's why phone companies are still mad at us for things we printed back in the 90s.

Dear *2600*:

A word in your blacklist is *not* blacklisted by Google: licked.

P

Stop the presses. This must have something to do with Trump gaining power.

Liberation

Dear *2600*:

Never underestimate what a motivated individual with a white van, uniform, safety vest, clipboard, and some orange cones can accomplish. Social engineering is not glorified much in *2600* culture, but we are the boots on the ground if you will. The art of obvious invisibility is learned and one must exercise to keep steady. This piece was always lusted after. Looking for phone booths. Happy hunting. Good Will.

massitakevin

We're not really sure what this was all about. The photos you sent us show most of the items you mention in an apparent phone booth heist (one photo shows it in place and the next shows it gone). It doesn't appear as if an actual phone was part of this operation, so it's likely that the piece that used to hold one was indeed abandoned. At least we sure hope so.

Dear *2600*:

I've avidly read *2600* for about five years now, and I'm loving every issue more and more - especially as my understanding of technology grows and I can better comprehend the material.

Always has this magazine warned of the dangers of governmental oversight, and draconian Internet laws. Never before 33:2 has it so clearly (to me) painted a startling picture of America being anything but a country of (at least some) technological liberty. Never before have I considered fleeing my home country.

Now that I'm thinking these thoughts, I am curious. What countries would you suggest I look at to move to, or what criteria should I use in finding a new hacker-friendly home? I don't even know where to start.

Thank you for any advice.

Sky

We've been getting this question quite a lot lately and it's totally understandable. But there are a few factors to consider. First, there is no place on the planet where you can escape the threats that are now at the forefront for us. Regimes change, people's attitudes can be manipulated, and what's abnormal this year can become the mainstream next year. Running isn't the answer. What is needed is for people to remain in their environment and do whatever they can to make it one they're comfortable in. It's your land, it's your flag, it's your culture just as much as it is anyone else's. By giving up, we cede all of that and make the job of our opponents so much easier. It's often difficult to stick around and so many of us are weary of fighting what can seem like an endless and fruitless battle. But we often don't see the victories or feel the progress that we've made. There are more people now who "get" technology, privacy, encryption, and how to become empowered than ever before. In a sense, it's good to have a fight in front of us because that's the surest way to realize the strength that we have. And there are so many examples of how this strength can be manifested: legal battles, publicity campaigns, disruption, direct actions, symbolic protests, and simply expressing oneself in writing, art, media, and fiction. You may find yourself in a place where none of that seems to matter. This is where people like you will count the most. The thing to remember is that you're not alone, the rest of us care, and your voice most definitely will be heard. Please don't be afraid to use it. History will thank you. And so will a lot of people in the present.

Scrutiny

Dear *2600*:

Changed your wiki page for "more accuracy" and "plainer language." Let's hope no one has changed it back by now. Y'all aren't the professional, uptight people Wikipedia made you seem like.

Oh, and my opinion on Trump: Julius Caesar once said, "He thinks too much. Such men are dangerous." Trump doesn't think his actions through, but at the same time, Mark Twain once said, "All you need in this life is ignorance and confidence, and then success is sure." Trump's ignorance to hackers and a lot of other things is outweighed by his confidence. Success is surely evident, unless of course America smartens up. But is Clinton really any better? Sure, she might not be a "threat" to you guys as much, but she's just as bad, just in different ways. The only hope is that we get through this together.

By the way, the three Bible-quoting cultists (Letters, 33:2) gave me a laugh. Talk about making a ministry!

(Sorry, the font changed. I can't get it back. Deal with it, like you dealt with my mistakes in my articles.)

NerveGas Jr.

We didn't notice your font change as we only read letters in ASCII. (It helps to eliminate distractions and give your actual words the weight they deserve.) We hope your font comes back to you. We don't know what you did to our Wikipedia page, but be aware that we have people on 24-hour standby who are alerted the second any misinformation is posted and spring into action.

We can't imagine what Julius Caesar would make of Trump, but Mark Twain would almost certainly have had a lot of fun with this. We know present-day writers certainly are.

Dear *2600*:

A couple of weeks ago, I purchased the latest two editions of *2600*. For diverse reasons, it was a long time since the last time I've done so (15 plus years).

Sadly to say, I have noticed an alarming decline in the quality of the articles. I consider most of them

too general/too vague or too trivial/obvious to add any real value. In two magazines, I've found only a couple of interesting/informative articles (I am assuming that the latest two magazines conform a good sample to infer the decline conclusion). This was not the case 15 years ago. Of course, this is not the editor's fault, but the lack of good articles coming to the magazine, as far as I understand.

I am not writing to you to criticize but to comment the following:

I've noticed that in recent years many interesting *freely available* talks like Defcon ones started to appear in the "recently" created YouTube. I am sorry to say that the content of many of those talks are far more interesting/informative than most of the articles I've found in the latest *2600* issues. I know this is *maybe* an unfair comparison, but the "market" of hacking knowledge changed in the last 15 years. I would rather comment that I don't know whether the number of *2600* sales is decreasing, increasing, or steady. As a matter of fact, I feel much more motivated to extract information from those talks than getting a *2600* magazine. Again, it's of course my personal view, but I suspect I am not the only one.

I guess that part of the decline of the quality of the articles (if there is so, maybe it's just my point of view) is because new generations of hackers are more focused on other communication channels to spread knowledge, like delivering talks that will be published on YouTube. Still, as in every science, written media is of most importance. So going to the point: Have you ever approached the guys that deliver talks in conferences like Defcon to propose them to write an article (based on the talk, perhaps)? I am asking because I don't know if it is possible or maybe you already tried. I guess that many are lazy enough to say no, but I bet that others will accept. According to my point of view, this will increase the quality of the material delivered by *2600*. Also, I am not sure if they receive money for the talk or not, but in most engineering conferences you don't.

In summary, it's just a thought and I hope this helps.

El Magistral

We do appreciate the observations and the critique. But it's hard to address your concerns without specifics. We do know there are great differences between putting on a talk and writing an article. The two aren't interchangeable without a good degree of work. But we have, in fact, done just as you suggested for the last few years and solicited speakers at our own conferences (which you don't seem to be aware of) to write articles and a good number have. Additionally, you don't seem aware of the fact that we've also been putting this material online free of charge for quite a few years. Visit Channel2600 on YouTube to see every talk presented since 1994.

Much can change over a decade and a half. Technology is certainly different and our own tastes and experiences also change with time so that an article we once found interesting no longer seems so. We've actually been getting such criticisms since our second year of publishing! But you do touch upon an interesting point with regard to trends and habits. Yes, people are more focused these days on videos than they are on reading. The entire publishing industry has been affected by this. We see far less zines on the stands than we have in the past, bookstores have disappeared entirely in many communities, and literacy seems to be less of a priority than ever. It doesn't have to be this way and we like to think that this hasn't happened to our many readers and writers. But it could be a bad sign for the future, which is why it's important to address these issues and work on ways to keep as many outlets as possible in existence. We all have the power to help here. Thanks for being alert to this and for engaging in the dialogue.

Electorials

Dear *2600*:

Am I the only one disheartened by Julian's announcement that he was timing the release of the Hillary docs to coincide closer to the U.S. election? I understand rationale and motives and all that, but at least WikiLeaks had the illusion of being above the political gaming, something of an anti-hero for the common man.... Now, just have to go back to question everything, even with the wiki... what is being released? What is the motive? Why? What is not being released? The narrative has changed....

machghostine

You're not the only one. Timing releases in order to have a specific effect is very different than releasing leaks as they come in. Of course, someone who leaks info can themselves time it for such an effect, but it would be profoundly wrong for a journalist to delay that release or to only publish material from one side if there was also material that could be harmful to the other side. If this election didn't prove the power we all can have simply by gaining/sharing access to bits of information, nothing ever will.

Dear *2600*:

The way I envision laws like the ones that put hackers in jail getting created and then forced upon its victims is not through politicians, but through lobby groups and corporations. Several corporations probably got compromised, most likely due to their lack of wanting to spend money on IT security than the absence of law. They decide to tell the lobby group they fund to push Congress to make the laws that benefit them and to also fund a cyber security entity so *they* don't have to. Of course, Congress rolls over and begs for the money while wasting taxpayer dollars on anything corporations desire.

In this election, we know which candidate gets the most contributions from Wall Street.

Nick

Most of what you say can be seen as fairly accurate, but conclusions aren't always that easy to arrive at. For instance, is it a foregone conclusion that someone who accepts more money from Wall Street will always be working for their perceived interests? It seems somewhat likely, but is it definite? Can we say with certainty that there couldn't be something a whole lot worse than this possibility? If, say, there was someone who didn't need Wall Street donations, was used to not playing by the rules, always got whatever they wanted, and lived in the fantasy world of corporations, do you think they would actually care more about the individual needs of the common people? Whatever the answer, we're in uncharted territory now. Enjoy the ride.

Dear *2600*:

I've always loved the magazine over the past 20 or so years. Was a bit "scared" to do a subscription. But hey, doubt that it's much on the radar these days with a hacker conference basically every weekend (and you guys keep things on the up and up legally - nothing too "dangerous").

But I gotta say, I'm kinda glad I didn't go to HOPE this year (and I *really* want to attend at least one in my life!). It seemed to have the same issue/problem the radio/podcast show has; it's *way* skewed towards political activism than hacking (radio considerably more so - conference this year seemed to be near a 50:50). Radio/podcast seems like a d-bag radio host talking "cyber." At times, seems the *Off The Hook* hosts are ten years behind what's going on in the trenches.

I do not want to be a complete curmudgeon. I watched (and *thank you!*) numerous talks live. I do applaud your effort. It's outstanding and about the best one can find for a U.S. hacker conference. And again, thank you!

I'm a multi-year mag subscriber, but can't really listen to the radio/podcast anymore (but love Bernie). Want to go to the next HOPE (need a New York pizza infusion - it and kKaiser rolls are the only thing I truly miss from New York).

Anonymous

You're certainly entitled to your opinion and we completely respect that. But anything that's countercultural by default has an element of political and/or social elements included. Our conferences have gotten wildly popular because of that, not in spite of it. And you clearly weren't able to resist it yourself! We don't want to be like other conferences, which, as you note, are fairly commonplace. In other countries, what we do is more the norm rather than the exception. So having that kind of a discourse here is absolutely essential and invaluable. We hear that constantly and our biggest complaint by far is that there isn't enough room. And after all that, there is still plenty of technical content. It's just that we're also looking at the bigger picture. Without groups like the Electronic Frontier Foundation, without fighting back on issues of encryption and content control, without exposing and battling the surveillance that is expanding all around us, we risk becoming little more than mindless consumers. As hackers, we deserve - and demand - better.

Our radio show follows a similar philosophy. For one thing, it's a radio show that also appears as a podcast. That alone makes it rather different than most podcasts, which tend to be narrowly focused to specific interests. When on the radio, there are millions more in the potential audience, many of whom weren't specifically searching for the content they're now being exposed to. That means the content needs to remain accessible to them by not becoming overly technical or designed for a niche, and by relating to other aspects of life. That includes the social and political ramifications.

There have always been people who want us to ignore the world around us and just focus on the technology. That has never been our purpose, not from our very first issue, our very first radio show, or our very first conference. If we were to do that, we'd basically be entrusting all of these vital issues to "experts" or people who allegedly cared, while we'd simply play with and talk about our toys. That may be how the mainstream views hackers. We see our culture as far bigger and far more vital to society at large.

Dear *2600*:

Your article against Trump is wrong to imply Trump is worse than Clinton. Her husband began the war on hackers from the PGP prosecution of Zimmerman, FBI's Carnivore, the DMCA, the Clipper Chip, and more. She and her party have been tarnished by hackers leaking their emails; now she has a strong incentive to crack down on hackers. Her privacy policy is *no different* than Trump's. She said, "It doesn't do anybody any good if terrorists can move toward encrypted communication that no law enforcement agency can break into before or after" while calling for a "Manhattan-like project" to break encryption. Like Trump, she also wants to shut down parts of the Internet. She said, "We're going to have to have more support from our friends in the technology world to deny online space." Invoking the Orwellian spirit of George Bush, she continued, "You're going to hear all of the usual complaints, you know, freedom of speech, etc. But if we truly are in a war against terrorism, and we are truly looking for ways to shut off their funding, shut off the flow of foreign fighters, then we've got to shut off their means of communicating." The only difference between Trump and Clinton is that Trump speaks more bluntly about what he believes due to being inexperienced at silver-tongued politics. But he and Hillary Clinton (and Bush and Bill Clinton) agree on this: statist encryption backdoors for the feds and totalitarian Internet censorship.

David

You'd be hard pressed to find a leader in the White House who didn't spout the above rhetoric. Go back over the past 30 years (beyond that it becomes harder to imagine how presidents might have dealt with today's technology) and ask yourself if any president wouldn't have wanted these kinds of capabilities. Look at other world leaders and see how many of them honestly care about people's privacy more than being perceived as able to always monitor the bad guys. We don't condone any of your examples and never will. But we do recognize that, bad as certain people and positions are, things can always be worse. And through our broken electoral system, we've just handed all of this power to a grossly incompetent corporate executive who spouts hatred at every turn and has abused every bit of power he's ever held. But even if you believe that he'll somehow see the light and not do everything in his power to crush individuals like us, take a good look at the people he's bringing in. They range from white supremacists to anti-science zealots to hard-liners who embrace torture as a law enforcement tactic. They are not our friends. And while there's plenty to criticize the Obama administration for, by far the biggest critique we're hearing is that they helped build an apparatus that could be extremely dangerous to freedom and liberty if it fell into the wrong hands. And that is precisely what has just happened. We've been warning about just such a scenario for many years. Now we get to see exactly how paranoid we really are.

Dear *2600*:

The election is right around the corner and *2600* has declared its support for Hillary. However, it makes no sense for hackers to support either Hillary (remember her Manhattan Project to break encryption) or Trump. Hackers who really value freedom should be voting for the Libertarian candidate. Libertarians will be much more accepting of personal liberties and privacy than either Democrats or Republicans. You can't have freedom and a nanny state at the same time. True freedom is personal freedom and economic freedom. The creativity of hackers, business people, and others is being suffocated under our nanny state of over regulation. The government is hopelessly in debt after decades of borrowing and spending to support military adventures all over the world and massive social programs at home. The Great Society has become a giant bloated pig being sucked dry by piglets sucking at the federal tit. In the 30 years from 1945 to 1975 we went from propeller planes to jets, we built the interstate highway system, sent a man to the moon, created modern computers, developed nuclear power, transformed agriculture, and were proud of the accomplishments. As a kid, I watched the space shuttle take its first flight, was promised bases on the moon, human exploration of Mars, and an extended life span. What did I get instead? Well, in the 30 years since, we have retired the space shuttle, we beg the Russians to take us to the ISS, our infrastructure is crumbling, the country spends a third of its budget on interest to service the national debt, free speech is under assault on college campuses, we've been told we have no right to privacy on our computers, the middle class is declining, and I will never see that human trip to Mars in my lifetime. What a waste of 30 years. If I sound pissed it's because I am. I work hard and I do well personally. But others need to do the same. We need new ideas in Washington and we need them now. No more endless welfare, military adventures everywhere, and mass uncontrolled immigration (culture matters). No more group based whiny identity politics. Let's get it together as a nation, build things again, explore the universe, be proud of our accomplishments, and fight for a culture of freedom and liberty. Vote differently this year. Shake things up and put some Libertarians in office! I don't agree with them on everything, but it can't hurt to have a third party to keep the two dominate parties a little more honest.

Piss Off Voter

You must have gotten a fake issue as we don't recall ever endorsing anyone. What we did was warn people against putting Trump in office and we stand by that. While many of your priorities are great, you must realize (and obviously, your letter was written before the election) that the way the system is set up, third party candidates have no chance of winning. That's not saying we shouldn't support them. But in this particular case, voting for them wasn't helping them. The goal was to keep a tyrant out of the White House. That goal failed. But in so doing, we may have opened the door to opportunity because never before have people realized how flawed our system is. Changing some of the fundamentals, coming to terms with the fact that rules can change over the centuries, and embracing a pro-democracy movement in this country where one person's vote is exactly equal to another's - these are goals that may at last be attainable if people use their anger and frustration to force change. That's when third parties can actually benefit. What many failed to realize on Election Day was that a vote isn't the equivalent of taking a jump shot where you either get what you want or you don't. It's more like a game of chess where a move might result in a painful sacrifice that can pay off down the road if you only think it through.

Dear *2600*:

First off, I feel I must use a Yahoo address to do this correctly. As I write this to you, my body is shaking. I'm so disgusted. For the last few years, I have picked up your rag for an occasional glance when I'm bored. I never really knew why. Your articles are always vague at best describing exploits. Nothing new is ever buried in them. There is never anything fantastical. Maybe it is for reflection of

things I've done or situations I've been in. Thanks to the last issue I know why. It is an escape from the sad reality that we as humans are in our twilight time in this thing we call the world, society, existence, etc.

I bought your rag and tossed it with some catalogs in the bathroom. I picked it up later as I was relaxing after a nice shit and opened it up to your rant about the election. I wish I never did that. As I read your rant, my pulse boiled and you ruined my day. I will never be able to innocently pick up your rag again. You have gone the *Wired* route. The every newspaper in America route. Except you do not disguise your commentary as news (I give you credit for that).

As a tinkerer with anything mechanical, digital, or whatever (I'm not a hacker), I step back and observe how things work. I have a very social job and you would not believe me if I told you what I do. But *I fucking hate Hillary Fucking Clinton*. Yes, I hate Obama and Bush too. I'm not a Republican, Democrat, or any other an, crat, ist. I'm a human living in a place other humans call *America*. I have not and never will have a Myspace, Facebook, Google, or any other socialist account. In my line of work, that is impossible and you should see or hear the people who ask for my contact account. If you took RTF in the 80s or 90s, you should be aware of FCC rules. They were very strict and allowed one station in each market and never the monopolies of media we have today. The same ones that are making up your mind and determining the election. The same ones using hate to get Clinton in office. Bill made that all possible in the 90s and the media owes him big time for it.

The UN or world order is taking your freedom and stepping in it as well. You have rich evil people like Soros and Koch spending money to divide us. Trump seems to be pissing a lot of people off and to me that is the hacker candidate. I'm not a white trailer person and I hope he wins. I know he will not though. The sheep are blindly biting the one thing that could be good for them as they eat all the poisoned oats. I'm so disgusted that you took away a small oasis from our forced propaganda machine and became part of it. Your days are numbered just like the human race. You would be amazed how many feel the same.

Bc smith

Ladies and gentlemen, the future.

Dear *2600*:

We all are overly familiar with the ease at which electronic voting machines are unreliable.

We are also all aware of the Russian government interfering in the United States' most recent election from start to finish.

I've created an online petition asking President Obama to do his duty, and defend the Constitution from this most egregious attack.

The text of the petition is below.

The link to sign it is: https://petitions.whitehouse.gov/petition/defend-constitution-and-united-sta tes-america

The petition reads as follows:

"We call on President Obama to act upon his Oath of Office, and use his powers under the War Act, the Patriot Act, as well as existing treaties and federal law to take immediate action regarding the most recent election. Today, we the people received further proof that the Russian Government has interfered repeatedly in our Federal Elections from the beginning of this election cycle. By doing so the Russian Government has committed clear Acts of War against The United States of America. We call on you to protect The Constitution and The United States of America, by setting aside the entirety of the 2016 Election, and calling for new elections AT ONCE."

No matter who you voted for, it is essential to our democracy that another State not be allowed to influence the outcome.

I hope you will help defend freedom. Thank you.

Stymtex

Let's take it down a notch, shall we? Even if Russia had interfered (and we're not saying they did), can you really be surprised? How often has the United States interfered in foreign elections? Who wouldn't want to launch a good disinformation campaign aimed at us? If there is fault to be doled out here, then it should go to the people who allow themselves to be manipulated in one direction or another. We're used to the media lying to us. We're used to the government lying to us. In fact, we always assume we're being lied to. Apart from infusing us with a real cheery attitude, this means that we're forced to actually do some of our own investigation and fact checking. It's really not that difficult. And if you care about what your choices are, you'll find a little extra time to do this. Otherwise, you really don't have the right to complain when you discover the wool's been pulled over your eyes after you start driving down the highway.

Of course, if this petition succeeded, you'd probably start a war with Russia and a civil war simultaneously. That's one thing we haven't managed to do yet.

Dear *2600*:

The day after the elections, I was listening to *Off The Wall*, with the *2600* staff lamenting the Trump win and the Clinton loss, siding with the protesters. I found this both nauseating as well as hypocritical. We are all sick and tired of Wall Street, the banks, even the Political Elites intruding into our lives, giving away our jobs, open borders, NSA spying, health care that nobody can afford, etc. All of this was rejected by Donald Trump but embraced by Hillary Clinton. And yet you were siding with the anarchists during the broadcast. This was shocking to the least. Trump won. Live with it.

Stan B.

First off, you must be referring to Off The Hook *as* Off The Wall *airs on Tuesdays and we weren't psychic enough to predict what was going to happen that night. More importantly, we think it's sad for people to try and discourage or mock people who have legitimate questions and grievances. That is how this country was founded and if we had followed the advice to "live with it" when we knew something was wrong on countless occasions, we wouldn't have accomplished anything. You don't have to agree with the argument, but not respecting the process and the passion is flat out wrong. What exactly is hypocritical about taking a stand? And if you had listened to either radio program at any time in the past few decades, we doubt our concerns would have been so shocking. And here's a final thought to leave you with. Our weird system allows for someone who is more than two million votes ahead to lose the election. But that weird system also allows for the Electoral College to go against the candidate they're pledged to vote for. If that were to happen and Donald Trump got kicked out on his ass, would you listen to us if we told you to "live with it?" Would we be shocked to see you demonstrating against that result? Do you think we would expect you to just shut up? It's not essential to agree on the issues in order to respect the positions people take.*

Events

Dear *2600*:

We're trying to get people to register for a global Capture the Flag hack competition this weekend. Wondered how I could get this message out to *2600* readers?

Karl

We're a quarterly magazine, so this kind of quick turnaround is kind of incompatible with what we do. Our Twitter account (@2600) is probably better for such appeals. Anyone can send us a Direct Message and we'll try our best to accommodate.

Dear *2600*:

Maker Faire 2016 at the New York Hall of Science was incredible. The 3D printing and fabrication was very active with various plastic or metal options. I may have seen the tone struck child who had to know the mystery of those tones. So many varied crafts in addition to purely electronic fabrication were also enchanting to open minds. People lit up and were naturally friendly.

Sometimes it can feel like everything is pretend, especially with the presidential racing. The Faire was a refreshing outdoor and indoor adventure of the minds. If you like to make things and/or see how they work, by all means please do go. That is my babbling fist-pump endorsement of Maker Faire and any more science-making.

Pic0o

We quite agree that these are really healthy outlets for anyone interested in learning. The Maker Faire people do a great job encouraging experimentation and questions, which is why they've become so fantastically popular with kids. This is an example of how applying the hacker mindset to a project can be incredibly beneficial. A more corporate approach simply wouldn't yield the same kind of results.

Digital Editions

Dear *2600*:

Thanks for putting on The Eleventh HOPE. I quite enjoyed myself. Thanks for also printing my photo of a telephone in Argentina in your Spring issue. It was quite a surprise. I just got a new job programming in Clojure, which is a LISP, so after getting some more experience at work with the new language, I'd love to submit an article on the history of LISP and a basic how-to of Clojure.

Since my best friend introduced me to *2600*, I've started by reading the digests. I see that Digests 1 to 3 and 25 to present exist in the Kindle store (I've purchased them all), but your *2600* online store is more up to date with your digital archiving efforts, having Digests 5 to 11.

I'm curious if you'll be releasing Digests 5 to 11 soon on Amazon, and also what the release plan is for the digests between 11 and 25. Hopefully, Kindle is still in your release plans. I love reading the back issues on my Kindle.

skilbjo

We're glad to hear you're enjoying the digests as we're putting in lots of time to get them right. We hope people seriously consider subscribing to the Hacker Digest Lifetime plan, which will eventually yield every issue ever printed in digital format. We spend a lot of time going over the old issues, explaining what was behind every cover, and highlight all of the various milestones we passed with every year. It's especially interesting in our first couple of decades, where there are so many parallels to what's happening in the present day, albeit with technology that is so very different.

To answer your question, we do intend to release everything on every platform. The Kindle requires much more work, however, as we need to OCR and proofread every line on those versions. So for now, we're simply scanning, adding content, and releasing a new digest every three months. By the time you read this, we'll be up to Volume 13 (1996). In a couple of years, we will have closed the gap and all of our material will be available in digital format. At that point, we hope OCR technology will have improved enough for us to tackle each year for the Kindle and other formats.

We look forward to seeing your article.

Dear *2600*:

I'm trying to buy the Kindle edition subscription of the magazine, but I get the message "...we did not find a Kindle device or reading app registered to your Amazon account for which this content is available."

I contacted Amazon support and their representative explained that the limitation is to devices. I read using the Kindle Cloud Reader. Individual magazine purchases and readings work without any problem using this "device." Why are Kindle edition subscriptions not allowed for the Kindle Cloud Reader? Do you plan on allowing Kindle Cloud Reader users to purchase the Kindle subscription in the future? If so, when?

Thanks in advance.

Huckle Buck

If it were up to us, it would be working right now. But it's not. We don't know why Amazon doesn't tell people this when they ask these questions. Publishers have no control over these issues. We really wish we did.

Fun with Calendars

Dear *2600*:

I was thrilled to get an email asking for my address and an offer to send me five copies, as my photo was used in the 2017 Hacker Calendar!

Here is the funny part... yesterday I received a "card" from Royal Mail saying that there was an item for me with import duty due, and I have to pay around $4.70 import duty and the Royal Mail another $10 in fees for the pleasure of having them collect my money on behalf of Her Majesty's Revenue and Customs Service.

That is what we get for doing the "right" thing and putting a value on the customs declaration form. I would have much preferred to give *2600* my money than HM Customs and Royal Mail - there is no escaping it!

Anyway, the calendar is simply brilliant, and I was happy to see my photo of a "hacked" phone booth on the front. I have posted images of it (with links to the *2600* shop) on certain social media, including, ironically, a special "exclusive" closed group that is for so called "creative" people who use Google products.

Here is the post on Ello: https://ello.co/neilhoward/post/hcoaacfid68lvyra-nqnbg

Thanks again.

Neil

Thanks for sending us an amazing photo. And we're sorry about the whole import duty thing. Please let us know what we can do differently to prevent this sort of thing from happening again.

Dear *2600*:

I friggin love these calendars. I'd love ideas on how to frame the old ones. Do people just frame the entire calendar, capturing only the cover page, or is there another trick to it?

Chris

It really depends on your taste. The cover page isn't always the one people frame. Any of the 12"x12" photos can be carefully cut out and placed in a frame after, of course, removing the staples. Use acid free paper tape and matte board if possible. This, however, should only be done after the year has ended or your calendar may stop functioning properly.

More Dialogue

Dear *2600*:

Asus txt hack

Pablo

That's it? That's all you have to say to us? In fact, you didn't even write an email; you just stuck that in the subject and left the body entirely blank. This is what our communications have devolved to: people sending us Twitter-length messages, links, or monosyllabic grunts. So you're either warning us of our vulnerability to the Asus hack (thanks, but we're fine) or you're asking us for more information on it. Very well, then, here's the deal. A couple of years ago, some users of Asus routers were compromised and a text file was left as a warning which said, among other things, "Your Asus router (and your documents) can be accessed by anyone in the world with an Internet connection." This took place months after the company was warned about the vulnerability and, in typical fashion, they claimed it wasn't an issue and basically ignored it. The text file warnings finally got their attention, but not before 13,000 IPs were compromised. So that's it in a nutshell. Thanks for writing and for starting this conversation.

Dear *2600*:

Please read this urgently! I hope it's being talked about on *Off The Hook* or in the magazine. I have a huge rant that I have to express in this letter. I truly hate how we in the U.S. cannot have access to foreign television or foreign programs due to shitty copyright laws around the world. What I mean is that I am pissed off that Japanese governments/media corporations don't like people sharing their content with other foreigners on the net. Sure, I know why because it's free for me to watch a Japanese music video/TV program. I am truly worried about sites like www.animeseason.com and other anime websites that show anime films/programs that have been shown on Japanese television because maybe they will be taken down by dumb copyright strikes. And also why the *fuck* would any major media corporation really fuck with someone who *just* wants to open a fan website that has pictures and media information? My favorite fan site called www.AKB48-daily.blogspot.com got taken down for unknown reasons and I hate it sooo much!

What do you all really think about corporations shutting down fan sites or forcing them to pay a fine due to small or tiny bits of copyright bullshit?

josh cha

While we may not achieve the same level of lividity as you, we do find this sort of thing to be contrary to the ideals of free expression and the sharing of art. Unless someone is actually stealing another's work

and profiting from it, we see no reason to impose such draconian laws on people who are likely huge fans. The abuse of copyright by copyright holders is far worse than copyright abuse by the populace. We have situations where historical works of art are left to decay in warehouses rather than be shared because "rights" haven't been - and probably never will be - obtained. We've seen original video work ruined by being forced to substitute cheaper music for digital releases to replace those whose copyright fees are too high. Copyrighted images or sounds have to be excised from works of art even if they're a part of our everyday lives. We got a good taste of this mentality with last year's "SplotchGate." We could go on with more examples of counterintuitive rules that artists and consumers are forced to live with. They serve no one except those who pocket the ransom involved in their enforcement. It's time we changed the rules of copyright so that they benefit the creators and the consumers alike. Some basic concepts should include default settings where works are forever accessible in their original state after they're completed, where new copyright rules can't be added on once a work is finished (an example being works that were licensed for VHS but not DVD), where free sharing of material that would otherwise be completely unavailable is allowed and encouraged. None of this would have to change the bottom line for the creators; in fact, done correctly, it could vastly improve them.

The Bounty

Dear *2600*:

I'm a reporter who just came across the $10k reward tweet: (https://twitter.com/2600/status/781206788804845568).

I'm planning on writing a story about the bounty. What I'm curious about is: Have you consulted lawyers about the plan? What do they say about the legality of the bounty?

P

Yes, if you blinked, you might have missed it, but there was a period of time when we were offering $10,000 to anyone who gave us access to Donald Trump's federal tax return. The offer expired on Election Day. (The lawyers we consulted with described it as legally solid.) We find it incredible that this information somehow was never leaked by anyone, considering all of the other data that managed to make its way into the mainstream during the campaign. Now that the damage has been done, this raises an interesting question. Do people have the right to see this information now that the target is the alleged leader of the free world? We strongly believe they do. And while it has now become a whole lot more dangerous to possess and/or reveal this information, it is still vital that we learn the truth. As journalists, we will protect anyone who comes forth. Obviously, using anonymizing email services and encryption (our PGP key can be found in the "Submissions" section of our website) will be beneficial, but we will do whatever is necessary even if it's sent in the clear. This, as always, applies to any sensitive material.

Dear *2600*:

How can I contribute to the Trump tax return bounty fund?

Kurt

We received so many similar inquiries while this campaign was in progress. Had we actually gotten any promising leads, we would have pursued a crowdfunding option that would have allowed us to raise much more money towards this goal. Without that probability, it could have been a logistical nightmare and we didn't want people throwing their money at something that was likely not to happen. Hope is not lost - we just have to rethink the strategy now that the playing field has been mined.

Appreciation

Dear *2600*:

Twenty years ago, my father would give me your magazine when he would visit. At the time, he was living out of his car because of the divorce. As time passed, computers and the Internet were the only way we could connect with each other. What I learned from your magazine enriched my life and strengthened my family through tough times. I'm now a professor of social media and taking care of my ailing father. Thank you for everything. This ski hat is for him.

William

Thanks for those kind words and please make sure your dad knows how much his actions in sharing our magazine have meant to you. We all take the little things for granted far too much and you've reminded us how important they really can be.

Dear *2600*:

Just wanted to say how much I enjoyed the Summer issue, especially your Letters responses to the crazy and stupid teenagers. Pretty sure the email from "Pietro" was a joke reference to *System Shock*, however.

A. S. A.

You're making a gigantic assumption that the people you considered to be "crazy and stupid" were teenagers. As for missing the reference to a video game, we hope we can be forgiven for remaining in the real world perhaps a bit longer than was healthy.

Dear *2600*:

I bought one of your magazines some years back and now I want to get a computer science Ph.D. I want my thesis to be on circle CPUs. If you can please rehabilitate me so I can do those things, great! I think my investment can allow that. God bless and thanks.

John

If you're honestly depending on us to get you a Ph.D., you might be in for a rude awakening. And you believe we can do this based on your having bought one of our issues years ago? We must have made one hell of an impression.

Something New

Dear *2600*:

Hi fellow *2600: The Hacker Quarterly* readers! Please check out the following universal resource pool for security engineers, hackers, and pentesters: www.hackpool.is.

Stratman01

You may regret this. Our readers tend to take exception to sites that proclaim things like: "We are the superelite hackers" or that have sections such as "Post a Gig" with guidelines that say "Post a hacking gig such as breaking into a Facebook account or gmail inbox or Twitter handle or even an iPhone or Android phone" while sticking a price tag on all of these activities. This plays into the simplistic mass-media induced notion of hackers being able to do anything, so long as the price is right.

Dear *2600*:

In the following months, I will be launching an online magazine/blog related to privacy and cybersecurity, written in Spanish, and I have become curious about your position/policy regarding derivative works of articles posted in the magazine. In this case, I am interested in creating and posting a translation to Spanish of one of the articles featured in the magazine. Thanks in advance.

s1w4t

This isn't a problem at all, as long as attribution is given to the author and the magazine. Please let us know how it goes.

Issues

Dear *2600*:

I'm trying to download episodes of *Off The Hook* and it appears that there are issues connecting to your server. I was able to download episodes from 1988 and 1989 but nothing from any of the other years. I've tried to do so on multiple computers and multiple networks with the same result. Is there maybe an ftp server with access to these files or an alternative method of downloading the episodes? Thanks!

Longtime *2600* Supporter!
Marc

This was probably some sort of connectivity issue which could have occurred anywhere between your machine and ours. There is no difference between one year and another when it comes to downloading shows. You can grab shows through our ftp server (ftp.2600.com, login as anonymous, connect to the "/pub" directory, and look around), but that's on the same network as the website, so doing that won't solve any routing issues.

The Wonderful World of Meetings

Dear *2600*:

Hey, I've seen there are meetings but some have stars before the names. Are the meetings still relevant? I have to say it's pretty odd locations.

Bachelet Lab

You're saying all of our meetings are in odd locations? If by odd you mean public, then that's true. We don't hide and the entire purpose of our monthly meetings is to connect with the public and find new people. That's why we encourage them to take place in easy to get to public spaces and not behind closed doors of any sort. As for the stars, which some may know as asterisks, all you need do is go to the bottom of the list to see what they designate. Those meetings are the ones that take place on Thursday evenings instead of Friday due to the Sabbath in Israel. We hope that solves any mysteries.

Dear *2600*:

The location you have for the Memphis, Tennessee *2600* group closed earlier this year. Attached are two news stories announcing this.

Jeff

It saddens us to hear this. Having verified your account and not having heard from the Memphis meeting in a while, we have no choice but to delist them. If someone else wants to restart the meetings there, they can contact meetings@2600.com and follow the instructions (or visit www.2600.com/meetings for info).

Dear *2600*:

Dropping you a note to let you know that I tried to attend the Hong Kong meeting and didn't find anyone. Unless you have a contact for Hong Kong or some other info, I'm going to start doing some advertising and see if I can get things moving again out here. I'll be keeping the same meeting time and location, as obviously there must be some history behind that and I don't have a reason to change it.

I know of at least two stores selling *2600 Magazine* in Hong Kong, so there should be at least some readers!

Leon

That is precisely the right attitude and game plan that's necessary to keep the meetings going. Some meetings are big and continue on their own momentum, while others are much smaller and can disappear entirely if a couple of people stop being involved. This doesn't have to happen if others step in and pick up the torch. All that's required is for a couple of motivated people to show up in the designated place at the designated time while doing what they can to spread the word locally. We're here to get the word out to the rest of the world. Thanks for believing and we wish you luck.

Dear *2600*:

Please add Orlando to the official listing for *2600* meetings. It should go between Melbourne and Titusville in the Florida listings. No, I won't

be there unless someone emails me and specifically wants to arrange something, but enough people come to Orlando for conventions, conferences, and just family gatherings at Disney, that they might be looking to get together with other *2600* readers if they're in town on a First Friday. I've visited *2600* meetings in other cities when I've been on the road and was able to find a meeting listing. Let's give Orlando visitors a chance to get together too.

R

It's a nice idea, but that's not how the meetings work. We can't just start meetings in places we want them to take place in without having actual people who are going to them. Perhaps someone will be inspired now to start a meeting in Orlando, and will show up and email meetings@2600.com with updates so it will be listed officially. We'll keep our fingers crossed.

Dear *2600*:

I am interested in starting up a *2600* meeting group in Edinburgh, Scotland. I have recently been to one of these in London and thoroughly enjoyed the atmosphere. At the moment, the plan is to look around for interest, and most likely start meetings from January 2017. A website is currently under construction, after which I am planning on establishing a social media presence.

Please let me know if this is OK.

stmerry

It's more than OK. We currently have meetings in Glasgow, so this would be a nice counterpoint. Please keep us updated and let us know how the first few meetings go.

Dear *2600*:

The Washington DC (Arlington) meeting is at the Rock Bottom at the Ballston Commons Mall. However, the mall has been undergoing renovations and the restaurant is closed. Has the Arlington meeting moved and, if so, where?

P.S. Keep doing what you're doing in these tough times.

Braden

This is, in fact, true and the meeting is currently described as "homeless" with attendees being encouraged to monitor the #DC2600 hashtag on Twitter to get updates. If the situation isn't resolved by the next issue, we'll have no choice but to delist it. In the meantime, we hope people help out and work on finding a suitable location.

Observed

Dear *2600*:

Someone has the plate "FREE KM" in Toronto!

Funkfish

Assuming this is indeed related to the Free Kevin (Mitnick) movement, it only shows how campaigns can resonate and last for a long time. Never forget this when embarking on a just cause that many feel has no chance of succeeding.

Knowledge Lost

Dear *2600*:

Where have all the "philes" gone? When I started getting into the scene, it was during the BBS days. Every board had over a hundred "philes." Granted, a lot of them were basically the same, but there was still a lot of knowledge being shared. On any given day, one could find information about almost anything from PBXs to this new thing called Linux. People were glad to share things they discovered and life was grand.

Then one magical day, I finally convinced my parents to get dial-up Internet. After that, I discovered a whole new world. Suddenly I had access to more. There were hundreds of "hacker" sites and many more chat rooms on IRC. Then, as time went on, things started moving underground. As time went on, I moved away and found other things to occupy my time.

It wasn't until about ten years later that I got the itch again. Today the scene is quite different. All the "philes" from yesterday are gone. It seems like all that knowledge has been lost. Yes, I realize that "hacking" is illegal. Talking about past exploits is going to get you busted. But it seems to me that the community has lost something. The last time I was on a message board, it seemed like everyone just wanted to make fun of anybody who asked a question. For example, I asked what was today's version of Satan/Saint. You would have thought I asked how to hack Facebook. What happened to the community of people sharing knowledge?

Joe

What you say has an element of truth to it, but is also overgeneralizing. People have been mocked for asking questions since shortly after the first question was asked. We have battled the belief that knowledge needs to be hidden underground since our first issue. There's nothing new about any of this. But the scenery has definitely changed and the particular magic of those old days just isn't there anymore. But that doesn't mean that the quest for knowledge is any less passionate. The real problem is that we succeeded. Everyone now seems to be interested in those things that so few of us really cared about before. Playing with computers, writing code, figuring out security holes, and making free phone calls are all the norm these days. That doesn't change the fact that most people still are only following a formula and not actually experimenting and challenging on their own. Real hackers are always in the minority and will always have to fight misperceptions. But the quest, the spirit, and the sharing of knowledge haven't gone anywhere and will always be with us.

KBChat - Private, Encrypted Chat via KBFS

by Samuel Hofius

I recently found out about a service called Keybase through an online acquaintance who offered to provide me with an invite to be a beta tester for the service (which, at the time I'm writing this, is the only way to sign up for the service). Keybase, according to their website[1], maps your identity to your public keys, and vice versa. I've been interested in cryptography (and more specifically, encrypting communications between people) for a long time now, but I've never made time to properly research it and play with it. So when I was offered an invite to a service that seemed to make it simple to dive into encrypted communication, I jumped at it.

At some point along the way, I found out about a feature of Keybase called KBFS[2] (Keybase Filesystem). KBFS is described as a cryptographically secure file mount. It is similar to services like Dropbox, Google Drive, and others. There are, however, several key differences between KBFS and other cloud-based storage services, and I will go over a couple of them in this article. One big difference between KBFS and other cloud-based storage services is the fact that two Keybase users can share files with each other in a manner that is both private and encrypted. Another is that KBFS mounts very cleanly into your operating system. These are the two main points that make kbchat.sh possible.

Once the Keybase app is installed and logged in on your Linux machine, you will find your KBFS mounted at /keybase/. Within this directory you will find two folders: /keybase/public/ and /keybase/private/. You can access any Keybase user's public files (including your own) at /keybase/public/{username}/ (of course, you need to replace any text in this article that's in curly braces with the correct username). You can access your own private files at /keybase/private/

yourname}/. The real magic of KBFS (as it pertains to kbchat.sh) comes in when you access a shared folder between yourself and someone else by going to /keybase/private/{yourname},{theirname}/. Any files in this shared folder will be signed and encrypted with both users' private keys, making the files available securely to both parties.

The idea behind kbchat.sh is very simple. The script creates a file called chat.log within a shared folder between yourself and the person with whom you are chatting. A tmux[3] session is spawned with two panes. The top pane runs a 'tail -f' (follow) command on the chat.log, which displays the last 10 lines of the log, plus any new lines that are added to the file while the script is running. The bottom pane loops infinitely with the bash 'read' command, and reads your input into a variable. Once input is received, the value of that variable is appended to the chat log file along with the current UTC date and time, as well as your Keybase username. There's more to the script, as I've added some color to the usernames and the option to wrap text in *asterisks* to make it appear bold. I've also added an option to close down the chat by typing '!exit' (although the chat.log file stays in the shared folder of both users).

For now, kbchat.sh only supports Linux, so that is what I've focused on in this article. KBFS, however, supports Windows, Mac, and Linux. The code will be available on GitHub[4], and you're free to make any changes. Also please feel free to write your own script which brings this idea to other operating systems.

References

[1] https://keybase.io
[2] https://keybase.io/docs/kbfs
[3] https://tmux.github.io/
[4] https://github.com/kf5grd/kbchat

kbchat.sh

```
#!/bin/bash

####### -- kbchat.sh -- #######
# Written by Samuel Hofius
# Private, encrypted chat via KBFS
# Usage: ./kbchat.sh <user>
# where <user> is the user you're chatting with
##############################

# display help if no remote user was entered
if [ -z ${1+x} ]; then
        echo ""
        echo "KBChat - Private, encrypted chat via KBFS"
        echo ""
        echo "Usage: $0 <user>"
        echo ""
        echo "  user [required]:        keybase.io username to chat with"
        echo ""
        exit
fi

# make sure we're not running as root as keybase doesn't allow this
userid=$(id -u)
[ $userid == '0' ] && \
        echo -e "This script cannot run as root.\nExiting..." && \
        exit

# get keybase user
kbuser=$(keybase status |grep "Username" |cut -d":" -f2 |tr -d [:space:])

# write script that will be used for the top pane
cat > /tmp/top_pane_$1.sh << EOF
#!$(which bash)
touch /keybase/private/$kbuser,$1/chat.log
tail -f /keybase/private/$kbuser,$1/chat.log | sed \\
     -e "s/\($kbuser:\)/\o033[31m\o033[1m\1\o033[0m/" \\
     -e "s/\($1:\)/\o033[34m\o033[1m\\1\o033[0m/" \\
     -e "s/\*\(.*\)\*/\o033[1m\\1\o033[0m/"
EOF

# write script that will be used for the bottom pane
cat > /tmp/bottom_pane_$1.sh << EOF
#!$(which bash)
function cleanup {
    rm /tmp/top_pane_$1.sh
    rm /tmp/bottom_pane_$1.sh
    tmux kill-session -t kbchat_$1
}

while true; do
    echo -en "\rMessage: "
    read messg
    [ "\$messg" == '!exit' ] && break

    echo "[\$(TZ=UTC date '+%F %H:%M')] $kbuser: \$messg" >> \\
         /keybase/private/$kbuser,$1/chat.log && \\
         clear
done
cleanup
EOF

chmod +x /tmp/top_pane_$1.sh
chmod +x /tmp/bottom_pane_$1.sh

# set up tmux session
tmux new-session -d -s "kbchat_$1" "/tmp/top_pane_$1.sh"
tmux split-window -v "/tmp/bottom_pane_$1.sh"
tmux resize-pane -D 20
tmux attach-session
```

WORDS YOU CAN USE

WHAT THEY SAY:
"Do you know what time it is?"
"How long is this going to take?"
"I am in the middle of eating dinner"
"I just walked in the door."

You have the option of calling back, but it could save you time if you have a few minutes for me right now. When calling the IRS, there can be long hold times while you wait to speak to a representative.

If you wait to call back, it is unlikely that you will speak to me. I can have your account up in front of me right now.

It is usually to your advantage to get whatever the issue is resolved as soon as possible.

It may be very long since we last spoke to you. I don't want to miss out on this opportunity to speak with you.

My name is Mr/Mrs/Ms _____ and my ID# is xx-xxxxx.

(When authorized)- I am calling from the Internal Revenue Service regarding a federal tax matter.

WHAT THEY SAY:
"Who is this?"
"What is this about?"
"Who wants to know?"

We have to protect the security of your tax account by verifying your information. Can I confirm your address? And your date of birth? To ease any concerns that the taxpayer may have, provide the taxpayer with the last four digits of his/her TIN (Social Security Number/ Employee Identification Number). Then, request that the taxpayer verify the first five digits.

We need to verify these items to protect your confidential tax information. We are required by law to ask these questions before disclosing any account information.

You will also have to verify these items if you choose to call us back before anyone can access your account.

WHAT THEY SAY:
"Can you tell me what this is about first?
"I can't give that info over the phone."

You were selected by our computerized dialer for this outgoing call for a reason, but I am prohibited from discussing that before I can verify your information.

Telephone calls are made when there is no response to IRS notices or the response did not completely resolve the issue.

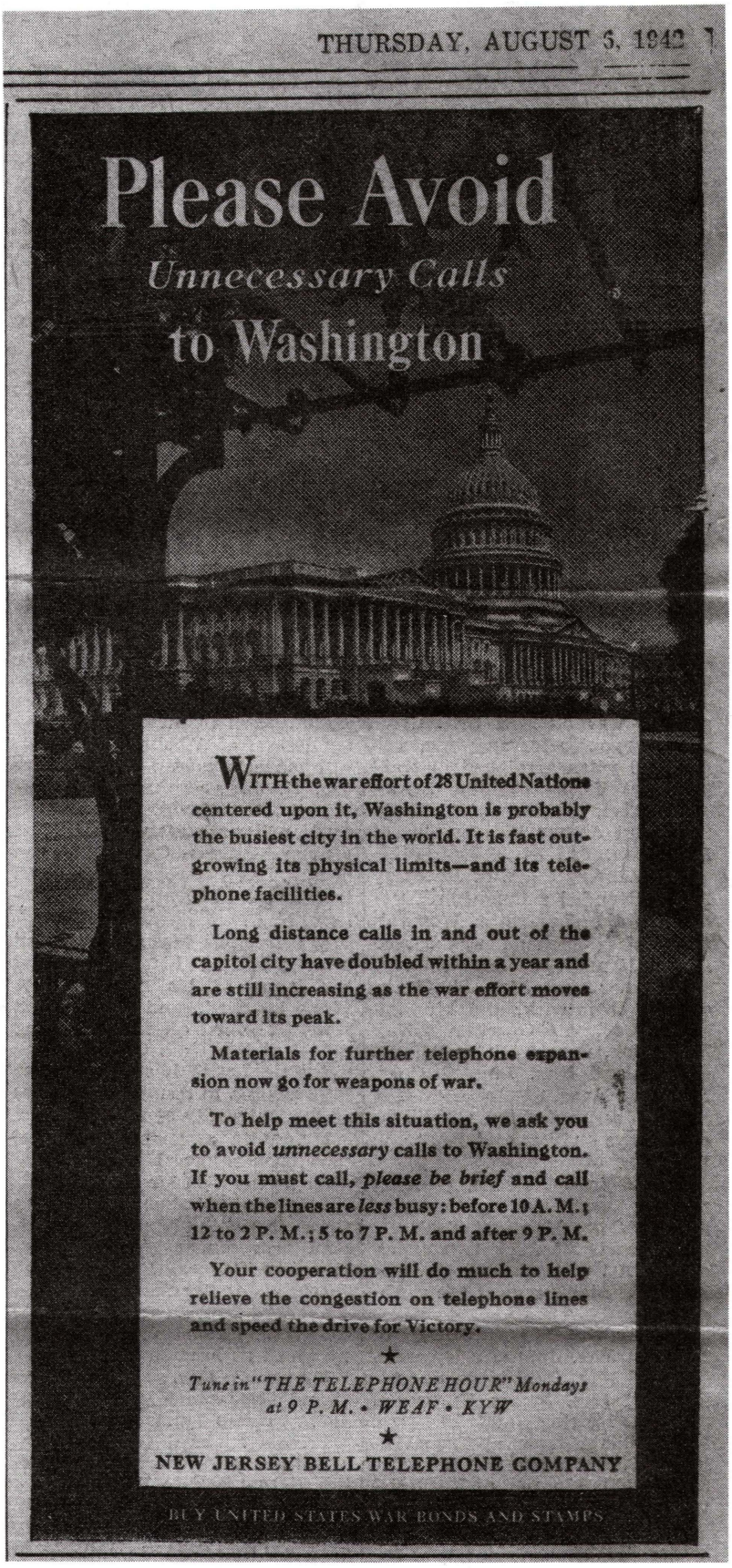
My job is to provide customer service to taxpayers to help them resolve their current tax problems and prevent future ones.

We may be calling because there has been a breakdown in communication somewhere. I can help you get that straightened out right now.

I can tell you about many programs that the IRS has to offer to assist taxpayers in financial trouble. Have you heard of our free file program?

WHAT THEY SAY:
"I have nothing to give."
"I am in over my head."
"I don't know where to start.

Got a leak for us? Email articles@2600.com and attach it!
(Our PGP key is on our web page under Submissions.)


THURSDAY, AUGUST 6, 1942
Please Avoid
Unnecessary Calls
to Washington
WITH the war effort of 28 United Nations centered upon it, Washington is probably the busiest city in the world. It is fast outgrowing its physical limits—and its telephone facilities.
Long distance calls in and out of the capitol city have doubled within a year and are still increasing as the war effort moves toward its peak.
Materials for further telephone expansion now go for weapons of war.
To help meet this situation, we ask you to avoid unnecessary calls to Washington. If you must call, please be brief and call when the lines are less busy: before 10 A. M.; 12 to 2 P. M.; 5 to 7 P. M. and after 9 P. M.
Your cooperation will do much to help relieve the congestion on telephone lines and speed the drive for Victory.
★
Tune in "THE TELEPHONE HOUR" Mondays at 9 P. M. • WEAF • KYW
★
NEW JERSEY BELL TELEPHONE COMPANY
BUY UNITED STATES WAR BONDS AND STAMPS

From New Jersey's Washington Star.

Submitted by Anne Jackson

EFFecting Digital Freedom

Five Things Tech Companies Must Do Before January 20

by Erica Portnoy and Elliot Harmon

Most of us won't soon forget where we were on Election Night, when the reality sunk in that Donald Trump would be the next president of the United States. Maybe you were in shock. Maybe you were in denial. Maybe you called a loved one to tell them it would be okay, or in hopes that they'd tell *you* the same thing.

Nobody knows exactly what will happen over the coming years, but we can tell you this: the tech community has a huge amount of power to steer things in the right or wrong direction. Tech companies can be complicit in a widespread assault on digital rights, or they can hold it back.

Let's be clear: the Electronic Frontier Foundation does not endorse political candidates. We *do* speak out about government restrictions on your digital civil liberties, no matter who's in office. If Trump tries to do half of the things he's promised to, it means that his administration will be turning to the tech industry to sell out its users. Big league.

Trump has promised to deport millions of our friends and neighbors, track people based on their religious beliefs, and undermine users' digital security and privacy. He's expressed a desire to "open up libel laws" and censor the Internet. But Trump can't carry out any of those plans without the tech industry's help. He'll need Silicon Valley's cooperation - and Silicon Valley can fight back.

In the next few years, we expect to see unprecedented demands on tech companies to hand over private data on people who use their services. This includes the conversations, thoughts, experiences, locations, photos, and more that people have entrusted platforms and service providers with. Under a hostile administration, that data could put thousands of people in danger.

If you manage tech that people rely on - everything from the smallest website to the largest software company - now is the time to put measures in place to protect your users.

Allow pseudonymous and anonymous access: Give your users the freedom to access your service pseudonymously and, ideally, with no login at all. Real-name policies are especially harmful to vulnerable populations, including pro-democracy activists and the LGBTQ community.

Stop behavioral analysis: Do not attempt to use your data to make decisions about user preferences and characteristics - like political preference or sexual orientation - that users did not explicitly specify themselves. If you do any sort of behavioral tracking, whether using your service or across others, let users opt out. This means letting users modify data that's been collected about them so far, and giving them the option to not have your service collect this information about them at all.

Delete your logs: Now is the time to clean up the logs. If you need them to check for abuse or for debugging, think carefully about which precise pieces of data you really need. And then delete them regularly - say, every week for the most sensitive data. IP addresses are especially risky to keep. Avoid logging them or, if you must log them for anti-abuse or statistics, do so in separate files that you can aggregate and delete frequently.

Encrypt data in transit: Does the ISP and the entire Internet need to know about the information your users are reading, the things they're buying, and the places they're going? It's 2016. Turn on HTTPS by default.

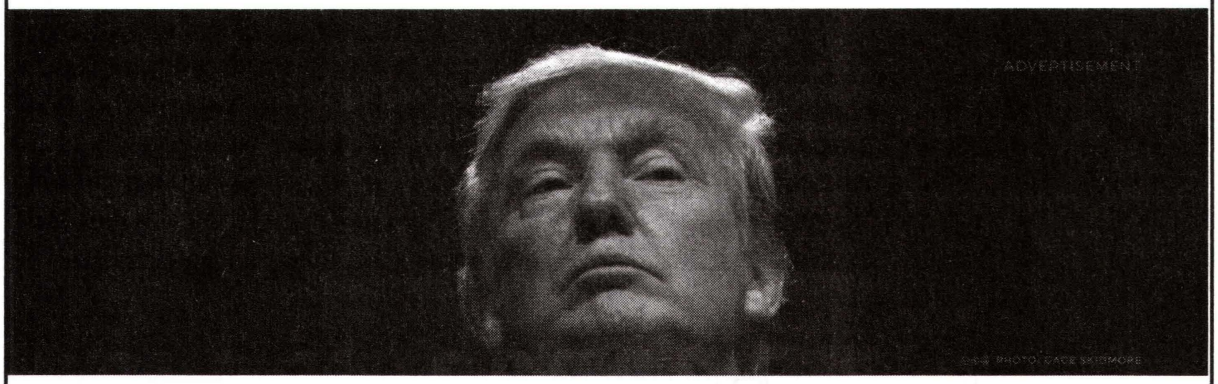
Enable end-to-end encryption by default: If your service includes messages, enable end-to-end encryption by default. Are you offering a high-value service - like AI-powered recommendations or search - that doesn't work on encrypted data? Well, the benefits of encrypted data have just spiked, as has popular demand for it. Now is the time to reevaluate that tradeoff. If it must be off by default, offering an end-to-end encrypted mode is not enough. You must give users the option to turn on end-to-end encryption universally within the application, thus avoiding the

dangerous risk of accidentally sending messages unencrypted.

These measures all boil down to respect for users' privacy. The best response to a demand for users' data is to say that you've got nothing, and mean it.

If you're like us, maybe you have another memory of Election Night. Maybe you got a dozen of those "Alice is on Signal" notifications as your friends and family finally decided to try that encrypted messaging app. Maybe you got a message from a friend asking you to explain how to send encrypted email, or what the name is of that program you use for browsing the web anonymously. Now is the time.

Whether you're a multinational tech company or just a geek with a laptop, you're on the front lines in the fight to protect people's privacy and security. If you'd like more information on how people can protect their own data, then visit our Surveillance Self-Defense guide at `https://ssd.eff.org`. If you'd like to get more involved with the fight for digital rights in your own community, then learn about our grassroots network at `https://www.eff.org/fight`.



TO THE TECHNOLOGY COMMUNITY:

Your threat model just changed.

Incoming President Donald Trump made campaign promises that, if carried out, threaten the free web and the rights of millions of people. He has praised attempts to undermine digital security, supported mass surveillance, and threatened net neutrality. He promised to identify and deport millions of your friends and neighbors, track people based on their religious beliefs, and suppress freedom of the press.

And he wants to use your servers to do it.

Today, we are calling on the technology community to unite with the Electronic Frontier Foundation in securing our networks against this threat.

ENCRYPT: Use HTTPS and end-to-end encryption for every user transaction, communication, and activity by default.

DELETE: Scrub your logs. You cannot be made to surrender data you do not have.

REVEAL: If you get a government request to monitor users or censor speech, tell the world.

RESIST: Fight for user rights in court, on Capitol Hill, and beyond.

When you stand with users, we'll stand with you. EFF has fought for the rights of technology creators and users for 26 years, through four different presidential administrations. As a nonpartisan nonprofit, we combine litigation, activism, and software development to defend civil liberties in the digital world.

The future of our democracy depends on an Internet that is free from censorship and government surveillance. Together we can ensure that technology created to connect and uplift people worldwide is not conscripted into a tool of oppression. Join us in defending users.

ELECTRONIC FRONTIER FOUNDATION

eff.org/defend-users

Rotten Apples: OS X 101

by Secure Panda
this.is.a.secure.panda@gmail.com

After reading Nervegas Jr's article in 32:4, I was mildly disappointed. The Apple computer is a thing of beauty and security, and especially in this time of intense debate about privacy and encryption, I feel it's important that people understand these machines in more detail. To this end, I propose to discuss the history and basic structure of the recent iterations of Apple's operating systems. I will also try to explain some of the security features that Apple now incorporates into their systems, and dispel some of the myths that are prevalent in the Apple community.

History 0x1

Apple's current operating system on both Mac computers and i-Devices is named Darwin, and is actually mostly BSD with some proprietary components. It evolved from NeXTSTEP, after Apple bought it in 1997. Starting with OS X in 2001, Apple has built all of its major OSes from this core Darwin kernel. Older versions were designed to run on PowerPC architecture, with Apple switching to Intel-based processors in 2006 and dropping official support for the older chips around that time. In 2007, the iPhone was released using a build of Darwin specifically for ARM architecture. For the "Modern Era" of devices that I'll be focusing on, this will encompass everything from OS X 10.6 to the present X64-based operating systems (as of March 2016).

Basic Structure 0x2

The system structure of Darwin is identical to most *NIX-based systems, for obvious reasons, and is usually not fully accessible on iOS. The root filesystem in OS X contains only four non-hidden folders: Applications, Library, System, and Users. Within the Users folder, each user on the system has a folder to contain their data, libraries, and settings. Starting with 10.7, the User library (~/Library) has been hidden, requiring one of two methods to get there (more on this later). With the release of OS X 10.11 (iOS 9), Apple introduced a new feature called SIP (System Integrity Protection) or KPP (Kernel Patch Protection) which introduces kernel checks. If the system fails the check (usually a hallmark of a jailbroken iOS device or a Hackintosh), then the kernel panics and halts.

Security 0x3

Nervegas Jr. already explained the "official" way to reset the password on a computer, and also went over how to enable the root user, as well as setting a firmware password using the recovery mode. What if I don't have a recovery mode (due to botched install or computer running 10.6 or earlier)? The solution is to use Single-User Mode! Start the computer up holding "Command" and "S" and it will bring you to a lovely CLI with a root prompt. Make sure you mount the drive, and you can reset any password or enable the root user from here.

```
mount -uw / #mounts the hard
➥ drive
ls /Users #lists all available
➥ users
passwd <user> #change the pass
➥word for <user>
passwd root #change the password
➥ for root, enabling it
```

This doesn't give you access to the passwords for that account. FYI: Apple secures all of that using a keychain file that's tied to your admin password. When you reset it, if you don't know the old password, kiss those saved passwords goodbye.

About that firmware password: it isn't that hard to get rid of. Change the amount of RAM in the machine, PRAM it twice, and you'll be able to get into whatever you needed into. This works on any version of OS X, and if you really can't figure out how to get into the machine, `iFixit.com` has detailed breakdown guides.

A quick note on FileVault, Apple's full-disk encryption: original FileVault isn't extremely difficult to remove from the computer. FileVault 2 (aka FileVault after 10.7) is significantly harder to get past. You can still erase the drive, but if you don't know the password or recovery key, you're out of luck. You'll have to take it to the store or call and deal with senior-level techs (who have to deal with engineering) to get it unlocked. This wouldn't be an issue, but 10.10 and later enables FileVault by default on laptops

that are plugged in during initial setup. This can be a huge headache for folks who don't have a backup but forgot their password.

Myths and Shenanigans 0x4

I hate people that claim Apple computers don't get viruses. They do, but because of Apple's market share (around four percent of computers worldwide), it's not usually worth the time of organized criminals to develop threats for these machines. The real threats to Apple occur from the use of the kernel for both X64 and ARM architecture: many of the vulnerabilities that exist within OS X will also exist in iOS.

iCloud is mostly secure. "The Fappening" happened because famous people used real answers to their security questions. If all someone needs to know to get access to your account is your mother's maiden name and the name of your first pet, you probably shouldn't answer those questions in public interviews, just sayin'.

Steve Jobs was a jerk. The whole world already knows it. Get over it.

Conclusion 0x5

When I first got into Apple hardware and software, I was not a big fan. I thought the computers were expensive, ugly things. After working with them for several years now, I've come to appreciate the effort that goes into making these computers. You can do just about anything on a Mac that you can do on a PC, but I'd personally prefer that more folks learn about their computers instead of swallowing the hype or ignorantly bashing something they've never used.

I'd like to do an article on iOS if I can find the time. The phones are simply fascinating, and the jailbreak community is fun and vibrant. Shouts to my wife and son (who despite my best efforts, can already navigate my iPhone at 2), my friends at Apple, and the folks who inspired me to write this. Props to Nervegas Jr. for the primer. Keep on Hackin'!

Automatic Contest Winning via Selenium

by Kyle Bradshaw

With some spare time on a recent weekend, my brain was begging for a project. Taking the opportunity, I remembered something I had wished existed in my teen years, and now realized the tools were available to create. Around 2010, I was addicted to Twitter, spending my time reading and responding to people I follow, and browsing tweets from certain search terms. Along the way, I began to win contests - lots of them! With prizes ranging from the usual t-shirts to my favorite: Japanese KitKat bars. One contest type I was really good at was code redemption, where a user tweets out an Xbox Live code for a game or DLC pack. I always had my redeem page open, ready to copy and paste. But I knew there had to be a better way.

Now, in my primary work time, I use the Selenium WebDriver to automate certain tedious tasks in a workplace situation. Usually, Selenium is used as a test suite for web dev projects, but it also works very well for our uses, because it does little[1] to give itself away as being automated, unless the site has advanced protection in place.[2] Having Python bindings just sweetens the deal for me. With my knowledge of this tool in hand, I set to work.

At this point, a little recon is in order, so we'll bust open IDLE and take a look.

```
import selenium
from selenium.webdriver.common.keys import Keys
# This is so we can press the Enter key later.

driver = selenium.webdriver.Firefox()
driver.get("https://account.xbox.com/en-us/paymentandbilling/redeemcode
➥/")
```

At this point, we're redirected to the login page. Let's make sure we can log in programmatically. Firefox makes this easy, right-click the Email Address box and choose Inspect Element. This

jumps to the relevant source code to identify the object. Already we can see that Microsoft is fighting back against us. So let's type something into the email and password boxes, highlight the text, and try to Inspect Element again. This gets us the ids "i0116" and "i0118" for the email and password fields respectively. So clear the boxes and let's try from IDLE:

```
em_box = driver.find_element_by_id("i0116")
em_box.click() # Just to be safe. Users usually don't
start typing in a box before clicking it.
em_box.send_keys("gil_baits@hotmail.com")
pw_box = driver.find_element_by_id("i0118")
pw_box.click()
pw_box.send_keys("password")
pw_box.send_keys(Keys.RETURN)
```

With valid info, this logs us in successfully and redirects back to the Redeem Code page. We're greeted with a shiny Redeem button. Let's Inspect it and send it a click.

```
rdm_btn = driver.find_element_by_id("redeemCodeBtn")
rdm_btn.click()
```

This is the home stretch. We can't quite as easily select the code box as we'd expect. Attempting to do so will return an error saying the Element can't be found. This is because Selenium treats web frames as separate web pages, and the frame we're looking for is nested rather deep.

```
driver.switch_to.frame("blenderIFrame")
driver.switch_to.frame("webBlendHost")
driver.switch_to.frame("appHost")
codebox = driver.find_element_by_id('tokenField')
codebox.send_keys("QQQQQ-QQQQQ-QQQQQ-QQQQQ-QQQQQ")
codebox.send_keys(Keys.RETURN)
```

Looking good! Now let's parse a given text for valid Xbox codes. We know that Xbox codes follow a given format: five sets of five alphanumeric characters. We can check for this easily using Python's regular expressions module, re.

```
import re
xbox_exp = re.compile(".{5}-.{5}-.{5}-.{5}-.{5}")
# . is any character, {5} indicates five of the previous character
def x_check(text):
    results = xbox_exp.findall(text.capitalize())
    # Capitalize it for our convenience.
    codes = False
    if len(results) > 0:
        codes = []
        for x in results:
            codes.append(x)
    return codes
```

Now we just need some text to run through our function. For this, the best source is likely Twitter, so using the available Twitter module, we can begin. For this you'll need valid Twitter API and OAuth keys for your account.[3]

```
import twitter
auth = twitter.OAuth(token, token_secret, consumer_key, consumer_secret)
stream = twitter.TwitterStream(domain="user
stream.twitter.com", auth=auth)
for tweet in stream.user():
    if "text" in tweet:
        x_check(tweet["text"]
```

Putting it all together into a complete automated process, we get CodeSnag.py, which I've taken the liberty of adding PlayStation support to and releasing,[4] making it ready for easy use and addition of new services. Now just follow those giveaway accounts, and rake in the winnings. Happy hunting!

[1] As of writing, only Firefox gives any signal that it's being run by a WebDriver, by setting the webdriver attribute in the HTML of every page.

[2] http://stackoverflow.com/a/33403473/955974

[3] https://apps.twitter.com/app/new

[4] https://bitbucket.org/Skylled/codesnag

The One about That File Server

by Sydney Greenstreet

This story has been around for so many years that it's probably been cast as having referred to every file storage system ever sold. The version that I was told attributed the event to a Novell arrangement. For me, it's inspired observations on everything from pre-Windows hardware resilience to support incident unpredictability to the ever-present lack of documentation that all will experience during one's next emergency/screwup/everyday work event.

Tech support gets a phone call. A user at a remote but nearby location can't get to their files (the ones stored remotely, not locally). Lots of things have already been tried: right-clicking rather than double-clicking at the icon in order to "run", several reboots, running any A/V, and so on. The user even looked at Task Manager to try to spot oddball processes or usage. Still, the normal result of the file window opening at the icon click and then showing folder icons wasn't happening. What resulted was a blank window with no files - and the user hadn't deleted anything. And no disk space info propagated at the window edge, either.

The support person then makes a house call to the user's location and sees the same set of results. Then it occurs to support that the location of the file server that this user stores work on is... uncertain. Not the path understood by software - the physical location of the box. Fortunately, a few other users stop by the cubicle and report the same issue that the first user gets. Those users don't know where the file server is, either. The admin who set everything up had retired two years earlier.

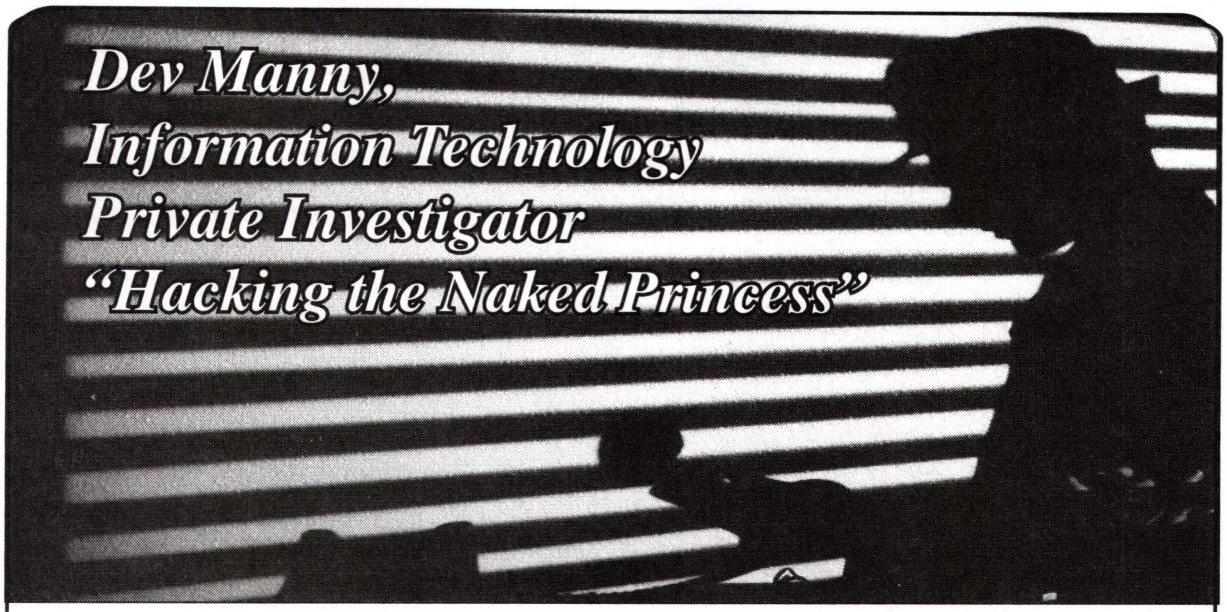
The support person's next hunch fails to help. A trip to the retired admin's networking room reveals all hardware up and running with all storage schemes responding properly to tests or at least pings. Notes are located that list the specific server holding the files of all the complaining users. The address looks good, but the box is nowhere to be found in the networking area. Whatever system was in use, it involved a wire going out the back of the user's workstation (RJ45, coax, token ring... whatever it was, the version of the story that I got wasn't specific) to the location of the server or its hub if applicable.

The support hero produces a flashlight and follows the wire from the user's desk behind several other desks across the office, tracking the progress of the wire (fastened to the baseboard) only to see it disappear into a hole drilled into the wainscoting. Support asks the office workers what's on the other side of the wall. They don't know. Some exploration with a tape measure leads around the corner and a closet is located in the opposite hall with a promising A/C vent in the door (looks like a server closet!) but nobody has a key to the lock and the key ring of the previous admin has no key that works. The building superintendent's keys don't fit either and a call goes out for a locksmith.

Hours later, the lock is picked, the door swings open, and out comes a cloud of dust, choking everybody. There's the file server! But the monitor has long since burned out and dust has to be wiped off just to see any switch position labels on the server case. Support goes looking for another monitor while the janitorial people bring up a vacuum cleaner. When the new monitor is hooked up, an error message appears, referring to a well-known repair utility. The utility is located on a 5 1/4 inch floppy in the networking room with "Novell" on the label. The floppy drive is vacuumed out for good measure, the utility is run for about ten minutes, a reboot ensues, and all files are available again for all users.

This story is useful to me in pointing out all kinds of aspects of technology then and now; the reliability of *nix-type systems; the wish that the old guy was still around to provide some arcane answer; the near-anarchy of the next service issue to hit the screen, phone, or chat system.... Do you really want to do this for a living? Sure you do. You'll see a lot of poorly tested, misconfigured, and oversold crap, but you also might see a system that's worked so well for so long that no user, admin, diagram, or supervisor can remember its location.

Dev Manny, Information Technology Private Investigator "Hacking the Naked Princess"



by Andy Kaiser

Chapter 0x12

Speeding down roads that my car had no business speeding on, I alternated between cursing my vehicle and myself.

I'd just dropped the most important bits of my case right into the hands of the person who shouldn't know them.

Oober, for all I knew, was not Oober. Or he'd hidden his true nature really well. Playing the role of a down-on-his-luck, emotionally-abused high school kid had worked well on me. Enough that I'd felt bad for him. Enough that I'd completely bought his story and shared confidential information.

He'd wormed his way into my case, and he'd used me to translate the clues from the Naked Princess into arrows pointing toward P@nic. P@nic, who needed to stay hidden from those who wanted to find her.

She'd trusted me. I was supposed to protect her. But I'd told Oober just what he needed to contact her, and he'd somehow used that info to find her.

As I swerved through intersections and lurched over bumps that I hoped were curbs, I replaced cursing myself with a more effective form of motivation: Using my anger to focus on learning and taking the next step.

I'd had plenty of evidence that Oober wasn't who he'd claimed to be. The connection to the Naked Princess. The confusion with his mom and dad. Twice as many hints as I usually got to work with, and I'd ignored them. That wouldn't happen again.

Lessons learned late are better than early,

(A horrible metallic grinding noise permeated my car.)

I won't forget pain when I'm feeling so surly.

There was a moral from this colossal snafu. And the moral rhymed, so, hey, bonus points. Anything to take my mind off the fact that I'd just clipped a fire hydrant.

I was getting close to P@nic's neighborhood of fancy mansions, immaculate lawns, and looming mortgage debt. I did the opposite recommendation of the nearest road sign, and slammed the accelerator to the floor. My car rewarded me with a few extra MPH and vomited the rest of my effort in a cloud of black tailpipe smoke.

I locked up my brakes trying to drift-spin into P@nic's street. My clattering, dented, hydrant-molested car caught disgusted glares from the neighborhood Teslas, Smartcars, and a refurbished DeLorean.

My car's engine sputtered and died from embarrassment, but I could see P@nic's home just a couple doors down, so I pushed out of my car and ran.

The front door was open a crack - that was always a bad sign - and I shoved it all the way open and entered through the foyer.

Next room over was a large family room. A comfy place, with a half-circle of laze-inducing furniture that angled towards a projector screen that spanned at least ninety inches.

On the screen was a collection of photos, clearly generated by the Naked Princess app. Some graphic and disgusting, some abstract yet weirdly disturbing, and some so nasty I took in a glance then looked away.

Oober and P@nic sat on the couch. Oober was slouching back, relaxed and comfortable, one hand behind his head, the other caressing a wireless keyboard. P@nic was sitting on the edge of the couch cushion, her back straight vertical and her mouth a flat horizontal. She was staring at the screen.

Oober glanced in my direction as I stumbled into the room, and spoke casually over his shoulder.

"Hey, Mister Information Technology Private Investigator. Let's talk about *you*."

He touched the keyboard and the screen changed.

I saw my own personalized Naked Princess photo, the overly-complicated Rubik's cube puzzle, expanded into glorious 90-inch detail.

"I've seen it," I said.

Oober frowned at the picture and then looked at me.

"That's it? What did you do to the program to get it to generate that? Give it random input? Lie?"

"Something like that," I said. "A lot like you did when we first met."

"Yeah," he smiled. It wasn't the sad, young, wistful smile I'd seen before. This smile was cold. Dead inside. "I screwed up my story, didn't I."

"It's hard to believe you were so abused, when the abuser changes from your dad to your mom. Especially after I'd just met your mom."

"Yeah. That. 'Mom' really isn't the best word for her."

"So what is she?"

"She's nothing. Let's get to what's important."

"Right," I said, moving into authoritative mode. "P@nic, let's get out of here. I can help you. We can -"

She was already shaking her head, and Oober was already smiling.

"No," she said. "I don't need to go anywhere."

"If this guy's threatened you, we can fix it."

She looked at me full in the face.

"He did. You can't. I'm fine."

"You don't look it. I can see your hands shaking from here."

"Reboot bought me out."

"Who?"

Oober pantomimed a sarcastic hat-tip.

"That's me," he said. "Reboot at your service."

"You're called Reboot? Or that's who you work for?"

He smiled.

"I don't have to tell you everything."

"No. But it would help."

"We'd been watching P@nic for a while. We saw the results we got from the Naked Princess. Give full credit to P@nic here," he said, giving her a nudge that earned him a glare. "She did a great job in the solution design. She'd already hacked through the social media APIs to get at the juicy big data, built the algos, and linked it all together with a seriously leveled-up understanding of psychology. All I needed to do was to get to the source code. After you led me here, the rest was just a question of cash, credit, or bitcoin."

"You know this won't work. It can't." I gestured at the screen, which was still showing off my personalized non-terrifying Naked Princess picture. "Bad data is too easy to collect and impossible to always filter out. You're gonna do what - use the Naked Princess as a picture generator to strike fear into your enemies? That's assuming your enemies all fill in their FriendyFace profile? Then what? People will freak out for a while, and just for a while, before they're desensitized. Show a kid a horror movie when they're young, and they'll be traumatized for a week. Then they assimilate and get over it. You're not going to accomplish anything!"

Oober - or Reboot - was nodding along with me patronizingly. He was nice enough to let me say my piece before he put my argument through the shredder.

"You might've been a part of this project, you know. You're okay at analysis and have a passable respect for reality. Except you've got it all wrong, man. You're thinking way too small. This is just a prank to you? Some social experiment gone wrong? A virus that needs to be stopped? No, you idiot, the Naked Princess is being weaponized."

"I don't see -"

"I know you don't. So shut up. We don't care about the photos. We don't care about the mental damage we're doing to all the precious snowflakes who are stupid enough to take everything they care about and put it online. Abusing that is easy, but it's a dead-end street. Like you just told me, the end game is already compromised. And like I just told *you, this* is about Big Data."

Reboot watched me and laughed.

"That stupid look on your face is why I'm a part of this and you're not. Spooky pictures were just a proof of concept. Step back and see another possibility. Using the source code, psychoanalysis, and data behind the Naked Princess, *we can predict what people will do, and we know what levers will force them to act.* From individuals to the masses, we know the future because we can make it happen. Stock market crashes, political elections and social revolts, hell, even something as simple as sports betting. Imagine what you could do if you had the power to influence these things, to know ahead of time, to stop them -"

"Or to start them."

"Yeah," he grinned. "That too. Very much. There will be damage. There has to be. But we'll use that damage and our influence to improve the world."

I looked at P@nic. Despite having been paid up into what I assumed was Officially Wealthy status by Reboot/Oober, she looked miserable.

Reboot caught the glance. He slapped his legs and stood up.

"I'm done here. I got what I needed. And you -" he stared at P@nic. "You got what you deserve, I suppose. Plenty of money and guilt. RedAction thanks you for your contributions to humanity."

He left.

P@nic and I stared at each other. There were tears in her eyes.

"You don't have to hide anymore," I said. "He's gone. You're safe."

"Don't you dare try and make me feel better. I know what this means. I don't know what I'm going to do. He said they'd pay me plenty and get out of my life. But if I didn't give them the source code, he said they would..." She swallowed.

"You didn't have a choice."

"How can I even report this? Who's supposed to help me? Can you?"

With a stab of guilt, I realized that P@nic didn't know about my mistake. She didn't know I'd led Reboot right to her. I'd find a way to tell her. Later. Maybe.

"You're not alone." I spoke with confidence I didn't feel.

"Well, then great. Here we are," she threw up both hands. "What are we supposed to do? There's nothing left. They gave me enough money to last me for life, and I don't even want it. It's dirty. They'll probably monitor how I use it, too, and keep me in a cage unless I drop completely offline."

"Well, that's not going to happen. We've got plenty to do before you should even think about going off the grid. I've got some ideas, thanks to our friend Reboot. I hope we never see the guy again, but something tells me we will."

"We will?" her face paled for a second, then anger flushed in her cheeks. "We will. We *will*. If you can fix this, I'm in. What's next?"

"Well, apparently there's the threat of social and political domination, so we might want to think about that at some point. But we just heard a name that makes me feel even worse."

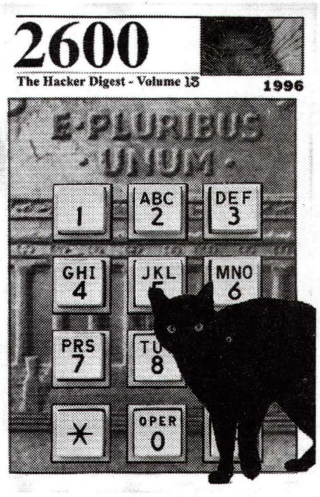
"What? Who?"

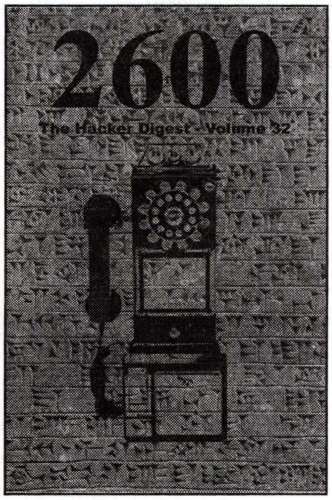
"Reboot just told us the name of his boss: RedAction."

"I don't know what that is."

"I do."

=== LIFETIME PDFs ===





Come and join the lifetime digital digest club. You'll get all of our existing *Hacker Digests*, plus a newly archived one every quarter, along with a brand new digest once a year for as long as you or we are around. $260 gets it all. (Analog lifetime subscribers can get this for $100.) Latest releases: Volume 32 from 2015 and Volume 13 from 1996.

Visit store.2600.com and click on Downloads/PDF.

HACKER HAPPENINGS

Listed here are some upcoming events of interest to hackers. Hacker conferences generally cost under $200 and are open to everyone. Higher prices may apply to the more elaborate events such as outdoor camps. If you know of a conference or event that should be known to the hacker community, ***email us*** at **happenings@2600.com** or by snail mail at **Hacker Happenings, PO Box 99, Middle Island, NY 11953 USA.** We only list events that have a firm date and location, aren't ridiculously expensive, are open to everyone, and welcome the hacker community.

January 13-15
ShmooCon 2017
Washington Hilton Hotel
Washington DC
www.shmoocon.org

April 1-2
Maker Faire U.K.
Life Science Center
Newcastle upon Tyne, England
www.makerfaireuk.com

April 14-17
Easterhegg 2017
Willy-Brandt-Halle
Mühlheim am Main, Germany
eh17.easterhegg.eu

May 4-5
THOTCON 0x8
Chicago, Illinois
thotcon.org

May 19-21
Maker Faire Bay Area
San Mateo Event Center
San Mateo, California
www.makerfaire.com

May 19-21
NolaCon
Crowne Plaza New Orleans
New Orleans, Louisiana
nolacon.com

June 9-11
CircleCityCon 4
Sheraton City Centre
Indianapolis, Indiana
circlecitycon.com

July 27-30
DEF CON 25
Caesar's Palace
Las Vegas, Nevada
www.defcon.org

August 4-8
SHA2017 Hacker Camp
Scoutinglandgoed Zeewolde
The Netherlands
sha2017.org

Please send us your feedback on any events you attend and let us know if they should/should not be listed here.

Marketplace

For Sale

NEEDFULWARES.COM. Thank you for your time today in reading this. Please visit this site to view the most beautifully hacked coins and hardcover books, handmade in the still-great USA! There are wonderfully handcrafted (some may called them hacked) coin rings (and book safes to hide them in) for EVERYONE. Yes, I make change into something you can wear on your body and books that will keep your wares (or whatever) safely hidden. These are great gift ideas and all my work has a Made-In-USA, money-back, no-hassle guarantee. Custom, handmade by myself, orders are available.

HTTP://CRYPTOBIZ.DIRECTORY. Show the world your professional side with CBD's comprehensive business identity package: profile page, email address, phone number, and document management solution for only .02 BTC, no verification necessary. Secured with Open Source software and hosted in a converted Swiss bunker deep inside a mountain. Your data and meta-data are safe here.

PORTABLE PENETRATOR. Find WPA WPA2 WPS Wifi Keys Software. Customize reports use for consulting. https://shop.secpoint.com/2600

HACKER WAREHOUSE is your one stop shop for hacking equipment. We understand the importance of tools and gear which is why we carry only the highest quality gear from the best brands in the industry. From WiFi Hacking to Hardware Hacking to Lock Picks, we carry equipment that all hackers need. Check us out at HackerWarehouse.com.

BLUETOOTH SEARCH FOR ANDROID searches for nearby discoverable Bluetooth devices. Runs in the background while you use other apps, recording devices' names, addresses, and signal strength, along with device type, services, and manufacturer. Handles Bluetooth Classic and Bluetooth LE (on LE-equipped Android devices). This is a valuable tool for anyone developing Bluetooth software, security auditors looking for potentially vulnerable devices, or anyone who's just curious about the Bluetooth devices in their midst. Exports device data to a CSV file for use in other programs, databases, etc. If you've used tools like btscanner, SpoofTooph, Harald Scan, or Bluelog on other platforms, you need Bluetooth Search on your Android device. More info and download at http://tinyurl.com/btscan.

CLUB-MATE is now easy to get in the United States! The caffeinated German beverage is a huge hit at any hacker gathering. Available in two quantities: $36.99 per 12 pack or $53.99 per 18 pack of half liter bottles plus shipping. Write to contact@club-mate.us or order directly from store.2600.com. WINTER EDITION now available!

GAMBLING MACHINE JACKPOTTERS, portable magnetic stripe readers & writers, RFID reader writers, lockpicks, vending machine jackpotters, concealable blackjack card counting computers, poker cheating equipment, computer devices, odometer programmers, and much more. www.hackershomepage.com

HACKERSTICKERS.COM has added tons of new shirts and lock picks for hackers, programmer and security geeks. Get a free sticker with purchase, just add to cart and enter "freestick" at checkout.

PRIVACYSCAN seeks & destroys privacy threats on the Mac wiping your tracks on where you surf and what you do on your computer. Learn more at http://privacyscan.securemac.com/

A TOOL TO TALK TO CHIPS. It's the middle of the night. You compile and program test code for what must be the 1000th time. Digging through the datasheets again, you wonder if the problem is in your code, a broken microcontroller... who knows? There are a million possibilities, and you've already tried everything twice. Imagine if you could take the frustration out of learning about a new chip. Type a few intuitive commands into the Bus Pirate's simple console interface. The Bus Pirate translates the commands into the correct signals, sends them to the chip, and the reply appears on the screen. No more worry about incorrect code and peripheral configuration, just pure development fun for only $30 including world wide shipping. Check out this open source project and more at DangerousPrototypes.com.

Announcements

COVERTACTIONS.COM is the place to find encryption products. Search by type, country, open source, platform, and more. Over 730 products listed with more added every day. Suggestions and feedback welcome.

AUSTIN HACKERSPACE: A shared workshop with electronics lab, laser cutters, 3D printers, CNC machines, car bay, woodworking, and more! $60/mo for 24/7 access to all this and a great community as well. Open House and open meetups weekly. 9701 Dessau Rd, Austin, TX http://atxhs.org/

SECUREMAC.COM IS BACK with the latest Apple security news! Submit your articles, writeup, and advisories. MacScan 3 was just released as well offering anti-malware protection for Mac OS X. Visit SecureMac.com.

HAVE YOU SEEN THE NEW *2600* STORE? We've finally made the jump into the 21st century with a store that has more features, hacker stuff, and endless possibilities than ever before. We now accept Bitcoin and Google Wallet, along with the usual credit cards and PayPal. We have more digital download capability for the magazine and for HOPE videos. Best of all, we've lowered prices on much of our stock. Won't you pay us a visit? store.2600.com

Services

GET YOUR HAM RADIO LICENSE! KB6NU's "No-Nonsense" study guides make it easy to get your Technician Class amateur radio license or upgrade to General Class or Extra Class. They are always up to date and clearly and succinctly explain the concepts, while at the same time, give you the answers to all of the questions on the test. The PDF version of the Technician Class study guide is free, but there is a small charge for the other versions. All of the e-book versions are available from www.kb6nu.com/study-guides. Paperback versions are available from Amazon, and an audiobook version of the Tech study guide is now available from Audible. E-mail cwgeek@kb6nu.com for more information.

DOUBLEHOP.ME is an edgy VPN startup aiming to rock the boat with double VPN hops and encrypted multi-datacenter interconnects. We enable clients to VPN to country A, and transparently exit country B. Increase your privacy with multiple legal jurisdictions and leave your traditional VPN behind! We don't keep logs, so there's no way for us to cooperate with LEOs, even if we felt compelled to; we simply respond with one liners from *50 Shades*. We accept Bitcoin and promote encrypted registration over Telegram Messenger. Use promo code COSBYSWEATER2600 for 50% off (https://www.doublehop.me).

DIGITAL FORENSICS FOR THE DEFENSE! Sensei Enterprises believes in the Constitutional right to a zealous defense, and backs up that belief by providing the highest quality digital forensics and electronic evidence support for criminal defense attorneys. Sensei's digital forensic examiners hold the prestigious CISSP, CCE, and EnCE certifications. Our

veteran experts are cool under fire in a courtroom - and their forensic skills are impeccable. We recover data nationwide from many sources, including computers, external media, tablets, and smartphones. We handle a wide range of cases, including hacking, child pornography possession/distribution, solicitation of minors, theft of proprietary data, data breaches, interception of electronic communications, identity theft, rape, murder, embezzlement, wire fraud, racketeering, espionage, cyber harassment, cyber abuse, terrorism, and more. Our principals are co-authors of *Locked Down: Practical Information Security for Lawyers, 2nd edition* (American Bar Association 2016), *Encryption Made Simple for Lawyers* (American Bar Association 2015), and hundreds of articles on digital forensics and an award-winning blog on electronic evidence. They lecture throughout North America and have been interviewed by ABC, NBC, CBS, CNN, Reuters, many newspapers, and even Oprah Winfrey's *O* magazine. For more information, call us at 703.359.0700 or email us at sensei@senseient.com.

LISTEN TO THE GREYNOISE PODCAST. There are many information security podcasts out there, and we're just one of them. We are here for the newbies and veterans alike! The greynoi.se podcast discusses general news, science, and privacy as well as technology specific issues, all from the hacker perspective. Recorded LIVE at the SYNShop Hackerspace in Las Vegas, NV, Friday nights at 7 pm. Recorded shows are usually online by Monday evenings. Have a listen and we LOVE feedback! https://greynoi.se

SECURE UNIX SHELLS & HOSTING SINCE 1999. JEAH.NET is one of the oldest and most trusted for fast, stable shell accounts. We provide hundreds of vhost domains for IRC and email, the latest popular *nix programs, access to classic shell programs and compilers. JEAH.NET proudly hosts eggdrop, BNC, IRCD, and web sites w/SQL. *2600* readers' setup fees are always waived. BTW: FYNE.COM (our sister co.) offers free DNS hosting and WHOIS privacy for $3.50 with all domains registered or transferred in! In memory of cheezi, aka Chris Holt.

SUSPECTED OR ACCUSED OF INTERNET-RELATED CRIMES? Stand up for your rights! Be polite, respectful, and calm. Repeat your own version of the following mantra: "Officer, I respectfully invoke all of my legal and Constitutional rights. Based on advice of counsel, I respectfully request to talk to my lawyer, I want to remain silent, and I will not consent to any search or seizure. Am I under arrest? Am I free to leave? Can I go now?" Omar Figueroa is an aggressive Constitutional and criminal defense lawyer with experience representing persons accused of hacking, cracking, misappropriation of trade secrets, and other cybercrimes. Omar is a semantic warrior committed to the liberation of information (after all, information wants to be free and so do we), and for more than a decade has provided pro bono representation for hackers, whistleblowers, and hacktivists. Past clients include Kevin Mitnick (million dollar bail case in California Superior Court dismissed), Robert Lyttle of "The Deceptive Duo" (patriotic hacktivist who exposed elementary vulnerabilities in the United States information infrastructure) and Vincent Kershaw (protester allegedly connected with Anonymous involved in a DDOS action against PayPal and member of the PayPal 14). Also, given that the worlds of the hacker and the cannabis connoisseur have often intersected historically, please note that Omar also defends non-violent human beings accused of committing cannabis offenses and also helps his clients understand the complex maze of medical marijuana-related laws and regulations in California. Please contact Omar Figueroa at (415) 489-0420 or (707) 829-0215, at omar@alumni.stanford.edu, or at Law Offices of Omar Figueroa, 7770 Healdsburg Ave., Ste. A, Sebastopol, CA 95472.

INTELLIGENT HACKERS UNIX SHELL: Reverse.Net is owned and operated by intelligent hackers. We believe every user has the right to online security and privacy. In today's hostile anti-hacker atmosphere, intelligent hackers require the need for a secure place to work, compile, and explore without big-brother looking over their shoulder. Hosted in Chicago with Filtered DoS Protection. Multiple Dual Core FreeBSD servers. Affordable pricing from $5/month, with a money back guarantee. Lifetime 26% discount for *2600* readers. Coupon Code: Save2600. http://www.reverse.net/

ANTIQUE COMPUTERS. From Altos to Zorba and everything in between - Apple, Commodore, DEC, IBM, MITS, Xerox... vintagecomputer.net is full of classic computer hardware restoration information, links, tons of photos, video, document scans, and how-to articles. A place for preserving historical computers, maintaining working machines, running a library of hard-to-find documentation, magazines, SIG materials, BBS disks, manuals, and brochures from the 1950s through the early WWW era. http://www.vintagecomputer.net

HACKERS, PHREAKERS, COMPUTER NERDS. Feel disillusioned, depressed, and dissatisfied with the way your life is passing? Need love, happiness, togetherness, and financial freedom? Here is the solution. Be with us to be yourself. You can be independent by joining with your kind. Enjoy the possibilities of collective thought, with associates who feel and think just like you do. Break that old routine, and dare to explore something new and unique. Contact THE HUB at: P. Bronson, P.O. Box 1000-AF8163, Houtzdale, PA 16698-1000.

DATA RAIN SOLUTIONS is a budding Colorado IT startup specializing in reliable and affordable remote tech support in advanced malware removal, PC optimization, diagnostics, and more. *2600* subscribers get 10% off their first order, as-need basis, or 1 year sub. Contact us: shanaroneasomi@yahoo.com. Visit us: http://shanaroneasomi.wix.com/datarain. Join the team! (Hackers welcome)

FBI FILES - Public service websites GetGrandpasFBIfile.com and GetMyFBIfile.com provide simple form letters to get dossiers from the FBI and other agencies. Free of charge. You can also print out the blank request templates if you prefer not to share personal information while using the website.

Personal

GOT TORPEDOED OUT OF THE FREE WORLD. Living in Fed world now, but would like to stay up on infosec, surveillance, and government oppression. I have written white papers on 4th Amendment issues, and would love like-minded people to correspond with and receive articles from. Kevin Reynolds, 59650-018, FCC Coleman-LOW, P.O. Box 1031, Coleman, FL 33521.

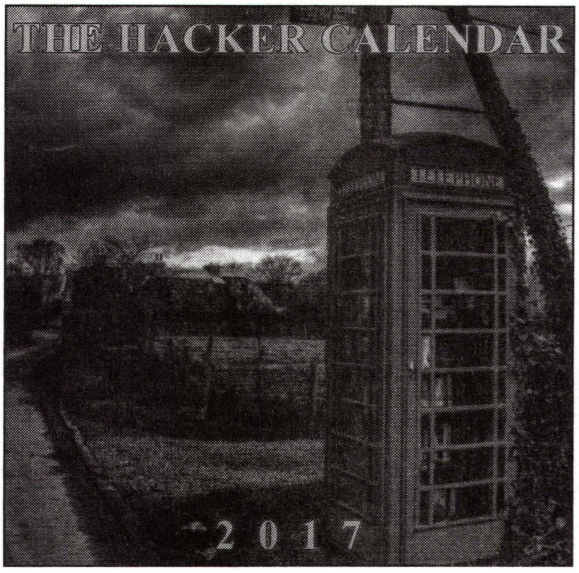
OPERATION PRISON PIRATE needs your help! OPP Media started as a hobby in 2012 to provide uncensored information and entertainment to various prisons in the U.S., but we've hit the limit of what we can do by ourselves. We really need donations. It costs us about $50 per broadcast, all out of pocket. Recently, our main transmitted was damaged, and we can't afford to replace it. We are also looking for engineers, producers, voiceover talent, or anyone who can help us in any way. We'd like to expand to cover even more prisons, but we need some help. E-mail us at OPPmedia@hushmail.com, and send bitcoins to 1J34tpXw84qM39LEZRtnUiVVpmuU6oxQJE.

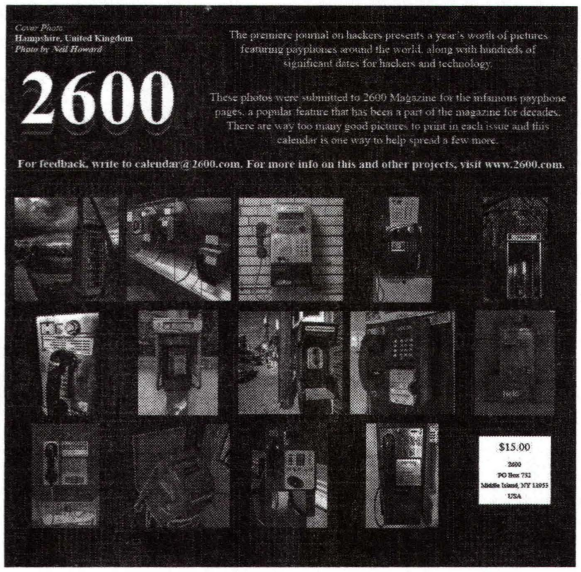
ONLY SUBSCRIBERS CAN ADVERTISE IN *2600!* Don't even think about trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. We make no guarantee as to the honesty, righteousness, sanity, etc. of the people advertising here. Contact them at your peril. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Don't expect us to run more than one ad for you in a single issue either. Include your address label/envelope or a photocopy so we know you're a subscriber. If you're an electronic subscriber, please send us a copy of your subscription receipt. Send your ad to *2600* Marketplace, PO Box 99, Middle Island, NY 11953. You can also email your ads to subs@2600.com.

Deadline for Spring issue: 2/21/17.

2017 HACKER CALENDARS

The 2017 Hacker Calendar is out! Each month features a 12"x12" glossy photo of a public telephone from somewhere on the planet, and nearly every day marks something significant in the hacker world.




Cover Photo:
Hampshire, United Kingdom
Photo by: Neil Howard
2600
The premiere journal on hackers presents a year's worth of pictures featuring payphones around the world, along with hundreds of significant dates for hackers and technology.
These photos were submitted to 2600 Magazine for the infamous payphone pages, a popular feature that has been a part of the magazine for decades. There are way too many good pictures to print in each issue and this calendar is one way to help spread a few more.
For feedback, write to calendar@2600.com. For more info on this and other projects, visit www.2600.com.
$15.00
2600
PO Box 752
Middle Island, NY 11953
USA

Get yours today! Only $9.99 at store.2600.com

ATTENTION LIFETIME SUBSCRIBERS!

If you want to receive annual digital digests instead of - or in addition to - your quarterly paper issues, this is now possible without having to buy both at full price. For $100, we will sign you up for the lifetime digital digest plan as well (once we verify that you are an existing lifetime subscriber). You will receive all of the digests that have already been released (Volumes 1-13 and 25-32) plus five newly released ones each year, and one per year once all of the back issue digests have come out. Just visit the downloads section at store.2600.com and sign up!

Since we take the word "lifetime" quite seriously, we will not cancel your existing subscription as long as you are still living. However, if you really don't want to get paper issues anymore, simply tell us this and you can transfer your subscription to someone else on our newly created lifetime waiting list. (It's like an organ donor waiting list but a whole lot more pleasant.) And you'll feel great having donated your remaining paper issues to someone who wouldn't have gotten them otherwise. Full details can be found at our store.

If the government is taken over by evil, hackers will be indispensable friends fighting for our freedom." - xphreak, 2600 Letters, Winter 1996-97

Editor-In-Chief
Emmanuel Goldstein

Associate Editor
Bob Hardy

Layout and Design
Skram

Cover
Dabu Ch'wald

Office Manager
Tampruf

STAFF

Infrastructure
flyko

Network Operations
phiber

Broadcast Coordinator
Juintz

IRC Admins
beave, koz, r0d3nt

Inspirational Music: Anugama, Wax Tailor, Barry McGuire, A Tribe Called Quest, Tune-Yards, Paul Haslinger

Shout Outs: Iron Feather Journal, Desus & Mero, Oceti Sakowin, DJ Qbert

_2600_ is written by members of the global hacker community. You can be a part of this by sending your submissions to articles@2600.com or the postal address below.

2600 (ISSN 0749-3851, USPS # 003-176); Winter 2016-2017, Volume 33 Issue 4, is published quarterly by 2600 Enterprises Inc., 2 Flowerfield, St. James, NY 11780. Periodical postage rates paid at St. James, NY and additional mailing offices.

POSTMASTER:
Send address changes to: *2600*
P.O. Box 752 Middle Island,
NY 11953-0752.

SUBSCRIPTION CORRESPONDENCE:
2600 Subscription Dept., P.O. Box 752,
Middle Island, NY 11953-0752 USA
(subs@2600.com)

YEARLY SUBSCRIPTIONS:
U.S. & Canada - $27 individual,
$50 corporate (U.S. Funds)
Overseas - $38 individual, $65 corporate

BACK ISSUES:
1984-1999 are $25 per year when available.
Individual issues for 1988-1999
are $6.25 each when available.
2000-2015 are $27 per year or $6.95 each.
Shipping added to overseas orders.

LETTERS AND ARTICLE SUBMISSIONS:
2600 Editorial Dept., P.O. Box 99,
Middle Island, NY 11953-0099 USA
(letters@2600.com, articles@2600.com)

***2600* Office/Fax Line: +1 631 751 2600**

Copyright © 2016-2017; 2600 Enterprises Inc.

MEETINGS

ARGENTINA

Buenos Aires: Bodegon Bellagamba, Carlos Calvo 614, San Telmo. In the back tables passing bathrooms.
Saavedra: Pizzeria La Farola de Saavedra, Av. Cabildo 4499, Capital Federal. 7 pm

AUSTRALIA

Central Coast: Ourimbah RSL (in the TAB area), 6/22 Pacific Hwy. 6 pm
Melbourne: Oxford Scholar Hotel, 427 Swanston St.
Sydney: Metropolitan Hotel, 1 Bridge St. 6 pm

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

BELGIUM

Antwerp: Central Station, top of the stairs in the main hall. 7 pm

BRAZIL

Belo Horizonte: Pelego's Bar at Assufeng, near the payphone. 6 pm

CANADA

Alberta

Calgary: Food court of Eau Claire Market. 6 pm
Edmonton: Elephant & Castle Pub, 10314 Whyte Ave, near big red telephone box. 6 pm

British Columbia

Kamloops: Student St in Old Main in front of Tim Horton's, TRU campus.
Vancouver: International Village Mall food court.

Manitoba

Winnipeg: St. Vital Shopping Centre, food court by HMV.

New Brunswick

Moncton: Champlain Mall food court, near KFC. 7 pm

Newfoundland

St. John's: Memorial University Center food court (in front of the Dairy Queen).

Ontario

Ottawa: World Exchange Plaza, 111 Albert St, second floor. 6:30 pm
Toronto: Free Times Cafe, College and Spadina.
Windsor: Sandy's, 7120 Wyandotte St E. 6 pm

CHINA

Hong Kong: Pacific Coffee in Festival Walk, Kowloon Tong. 7 pm

COSTA RICA

Heredia: Food court, Paseo de las Flores Mall.

CZECHIA

Prague: Legenda pub. 6 pm

DENMARK

Aalborg: Fast Eddie's pool hall.
Aarhus: In the far corner of the DSB cafe in the railway station.
Copenhagen: Cafe Blasen.
Sonderborg: Cafe Druen. 7:30 pm

FINLAND

Helsinki: Forum shopping center (Mannerheimintie 20), food court on floor zero.

FRANCE

Cannes: Palais des Festivals & des Congres la Croisette on the left side.
Grenoble: EVE performance hall on the campus of Saint Martin d'Heres. 6 pm
Lille: Grand-Place (Place Charles de Gaulle) in front of the Furet du Nord bookstore. 7:30 pm
Paris: Place de la Republique, opposite the empty fountain. 6 pm
Rennes: Bar le Golden Gate, Rue St Georges a Rennes. 8 pm
Rouen: Place de la Cathedrale, benches to the right. 8 pm
Toulouse: Place du Capitole by the benches near the fast food and the Capitole wall. 7:30 pm

GREECE

Athens: Outside the bookstore Papasotiriou on the corner of Patision and Stournari. 7 pm

IRELAND

Dublin: At the payphones beside the Dublin Tourism Information Centre on Suffolk St. 7 pm

ISRAEL

***Beit Shemesh:** In the big Fashion Mall (across from train station), second floor, food court. Phone: 1-800-800-515. 7 pm
***Safed:** Courtyard of Ashkenazi Ari.

ITALY

Milan: Piazza Loreto in front of McDonalds.

JAPAN

Kagoshima: Amu Plaza next to the central railway station in the basement food court (Food Cube) near Doutor Coffee.
Tokyo: Mixing Bar near Shinjuku Station, 2 blocks east of east exit. 6:30 pm

MEXICO

Chetumal: Food court at La Plaza de Americas, right front near Italian food.
Mexico City: "Zocalo" Subway Station (Line 2 of the "METRO" subway, the blue one). At the "Departamento del Distrito Federal" exit, near the payphones and the candy shop, at the beginning of the "Zocalo-Pino Suarez" tunnel.

NETHERLANDS

Utrecht: In front of the Burger King at Utrecht Central Station. 7 pm

NORWAY

Oslo: Sentral Train Station at the "meeting point" area in the main hall. 7 pm
Tromsoe: The upper floor at Blaa Rock Cafe, Strandgata 14. 6 pm

PERU

Lima: Barbilonia (ex Apu Bar), en Alcanfores 455, Miraflores, at the end of Tarata St. 8 pm
Trujillo: Starbucks, Mall Aventura Plaza. 6 pm

PHILIPPINES

Quezon City: Chocolate Kiss ground floor, Bahay ng Alumni, University of the Philippines Diliman. 4 pm

RUSSIA

Moscow: Pub Lora Craft, Pokrovka St 1/13/6. 7 pm

SWEDEN

Stockholm: Starbucks at Stockholm Central Station.

SWITZERLAND

Lausanne: In front of the MacDo beside the train station. 7 pm

THAILAND

Bangkok: The Connection Seminar Center. 6:30 pm

UNITED KINGDOM

England

Brighton: At the phone boxes by the Sealife Centre (across the road from the Palace Pier). Payphone: (01273) 606674. 7 pm
Leeds: The Brewery Tap Leeds. 7 pm
London: Trocadero Shopping Center (near Piccadilly Circus), front entrance on Coventry St. 6:30 pm
Manchester: Bulls Head Pub on London Rd. 7:30 pm
Norwich: Entrance to Chapelfield Mall, under the big screen TV. 6 pm

Scotland

Glasgow: Starbucks, 9 Exchange Pl. 6 pm

Wales

Ewloe: St. David's Hotel.

UNITED STATES

Alabama

Auburn: The student lounge upstairs in the Foy Union Building. 7 pm

Arizona

Phoenix (Mesa): HeatSync Labs, 140 W Main St. 6 pm
Prescott: Method Coffee, 3180 Willow Creek Rd. 6 pm
Tucson: Sunny Daze Cafe. 6 pm

Arkansas

Ft. Smith: River City Deli at 7320 Rogers Ave. 6 pm

California

Anaheim (Fullerton): 23b Shop, 418 E Commonwealth Ave (business park behind the thrift store). 7 pm
Chico: Starbucks, 246 Broadway St. 6 pm
Los Angeles: Union Station, inside main entrance (Alameda St side) near the Traxx Bar. 6 pm
Monterey: East Village Coffee Lounge. 5:30 pm
Sacramento: Hacker Lab, 1715 I St.
San Diego: Regents Pizza, 4150 Regents Park Row #170.
San Francisco: 4 Embarcadero Center near street level fountains. 6 pm
San Jose: Outside the cafe at the MLK Library at 4th and E San Fernando. 6 pm

Colorado

Fort Collins: Dazbog Coffee, 2733 Council Tree Ave. 7 pm.

Connecticut

Newington: Panera Bread, 3120 Berlin Tpke.

Delaware

Newark: Barnes and Nobles cafe area, Christiana Mall.

District of Columbia

Arlington: Rock Bottom at Ballston Commons Mall. 7 pm

Florida

Fort Lauderdale: Undergrounds Coffeehaus, 3020 N Federal Hwy. 7 pm
Gainesville: In the back of the University of Florida's Reitz Union food court. 6 pm
Jacksonville: Kickbacks Gastropub, 910 King St. 6:30 pm
Melbourne: Sun Shoppe Cafe, 540 E New Haven Ave. 5:30 pm
Sebring: Lakeshore Mall food court, next to payphones. 6 pm
Titusville: Bar IX, 317 S Washington Ave.

Georgia

Atlanta: Lenox Mall food court. 7 pm

Hawaii

Hilo: Prince Kuhio Plaza food court, 111 East Puainako St.

Idaho

Boise: BSU Student Union Building, upstairs from the main entrance. Payphones: (208) 342-9700.
Pocatello: Flipside Lounge, 117 S Main St. 6 pm

Illinois

Chicago: Space by Doejo, 444 N Wabash, 5th floor. 6 pm
Peoria: Starbucks, 1200 West Main St.

Indiana

Evansville: Barnes & Noble cafe at 624 S Green River Rd.
Indianapolis: City Market, 2nd floor, just outside Tomlinson Tap Room.
West Lafayette: Jake's Roadhouse, 135 S Chauncey Ave.

Iowa

Ames: Memorial Union Building food court at the Iowa State University.
Davenport: Co-Lab, 627 W 2nd St.

Kansas

Kansas City (Overland Park): Barnes & Noble cafe, Oak Park Mall.
Wichita: Riverside Perk, 1144 Bitting Ave.

Louisiana

New Orleans: Z'otz Coffee House uptown, 8210 Oak St. 6 pm

Maine

Portland: Maine Mall by the bench at the food court door. 6 pm

Maryland

Baltimore: Barnes & Noble cafe at the Inner Harbor.

Massachusetts

Boston: Stratton Student Center (Building W20) at MIT in the 2nd floor lounge area. 7 pm

Michigan

Ann Arbor: Starbucks in The Galleria on S University. 7 pm

Minnesota

Bloomington: Mall of America food court in front of Burger King. 6 pm

Missouri

St. Louis: Arch Reactor Hacker Space, 2215 Scott Ave. 6 pm

Montana

Helena: Hall beside OX at Lundy Center.

Nebraska

Omaha: Westroads Mall food court near south entrance, 100th and Dodge. 7 pm

Nevada

Elko: Uber Games and Technology, 1071 Idaho St. 6 pm
Las Vegas (Henderson): Las Vegas Hackerspace, 1075 American Pacific Dr Suite C. 6 pm
Reno: Barnes & Noble Starbucks 5555 S. Virginia St.

New Hampshire

Keene: Local Burger, 82 Main St. 7 pm

New Jersey

Somerville: Dragonfly Cafe, 14 E Main St.

New York

Albany: Starbucks, 1244 Western Ave. 6 pm
New York: Citigroup Center, in the lobby, 153 E 53rd St, between Lexington & 3rd.
Rochester: Interlock Rochester, 1115 E Main St, Door #7, Suite 200. 7 pm

North Carolina

Charlotte: Panera Bread, 9321 JW Clay Blvd (near UNC Charlotte). 6:30 pm
Greensboro: Caribou Coffee, 3109 Northline Ave (Friendly Center).
Raleigh: Cup A Joe, 3100 Hillsborough St. 7 pm

North Dakota

Fargo: West Acres Mall food court.

Ohio

Cincinnati: Hive13, 2929 Spring Grove Ave. 7 pm
Cleveland (Warrensville Heights): Panera Bread, 4103 Richmond Rd.
Columbus: Front of the food court fountain in Easton Mall. 7 pm
Dayton: Marions Piazza ver. 2.0, 8991 Kingsridge Dr., behind the Dayton Mall off SR-741.
Youngstown (Niles): Panara Bread, 5675 Youngstown Warren Rd.

Oklahoma

Oklahoma City: Cafe Bella, southeast corner of SW 89th St and Penn.

Oregon

Portland: Theo's, 121 NW 5th Ave. 7 pm

Pennsylvania

Allentown: Panera Bread, 3100 W Tilghman St. 6 pm
Harrisburg: Panera Bread, 4263 Union Deposit Rd. 6 pm
Philadelphia: 30th St Station, food court outside Taco Bell. 5:30 pm
Pittsburgh: Tazz D'Oro, 1125 North Highland Ave at round table by front window.
State College: in the HUB above the Sushi place on the Penn State campus.

Puerto Rico

San Juan: Plaza Las Americas on first floor.
Trujillo Alto: The Office Irish Pub. 7:30 pm

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Knoxville: West Town Mall food court. 6 pm
Nashville: Emma Inc., 9 Lea Ave. 6 pm

Texas

Austin: The Chicon Collective, 301 Chicon St, Suite D. 7 pm
Dallas: Wild Turkey, 2470 Walnut Hill Ln. 7 pm
Houston: Ninfa's Express seating area, Galleria IV. 6 pm
Plano: Fourteen Eighteen Coffeehouse, 1418 Ave K. 6 pm

Vermont

Burlington: The Burlington Town Center Mall food court under the stairs.

Virginia

Arlington: (see District of Columbia)
Blacksburg: Squires Student Center at Virginia Tech, 118 N. Main St. 7 pm
Charlottesville: Panera Bread at the Barracks Road Shopping Center. 6:30 pm
Richmond: Hack.RVA 1600 Roseneath Rd. 6 pm

Washington

Seattle: Cafe Allegro, upstairs, 4214 University Way NE (alley entrance). 6 pm
Spokane: Starbucks, Hawthorne Ave.
Tacoma: Tacoma Mall food court. 6 pm
Wenatchee: Badger Mountain Brewing, 1 Orondo Ave.

Wisconsin

Madison: Fair Trade Coffee House, 418 State St.

All meetings take place on the first Friday of the month (a * indicates a meeting that's held on the first Thursday of the month). Unless otherwise noted, *2600* meetings begin at 5 pm local time. To start a meeting in your city, send email to meetings@2600.com.

Follow @2600Meetings on Twitter and let us know your meeting's Twitter handle!

International Payphones

United Arab Emirates. The kind of phone you'd expect to see in an airport terminal in Dubai. As well as on Page 2 of this issue. ***Photo by AM (secuid0)***

Canada. In Scarborough, Ontario, you can actually find a phone booth that has a tree growing in it! Or at least you could. We're told the phone has since been decommissioned and removed.

Photo by David McLeod

Japan. We can't tell you what city this phone and accompanying phone card vending machine were spotted in. That's because the green pair pass through cities at 200 mph on the Shinkansen high speed train line.

Photo by Cobolt

Thailand. Another phone booth with vegetation and a good amount of color. Found in the Watthana district of Bangkok.

Photo by Robert Wood

Visit **http://www.2600.com/phones/** to see our foreign payphone photos!
(Or turn to the inside front cover to see more right now.)

The Back Cover Photos

Many of us have seen this particular New York City subway car - in fact, it even made it to one of our covers back in 2005 - and this is a shot from the inside, captured by **Robby R.O.B.B.** For those who want to find the "2600" car, wait around on the "D" line and it should eventually show up. (Please don't pull the cord.)

A really interesting story is connected with this cardboard box. **David Graper** tells us that Troy Typewriter in upstate New York was one of the few remaining typewriter repair stores left in existence. The guy who ran the place had a longtime reputation as a true hacker who respected the old technology and somehow managed to keep machines of all types running without proper access to parts or supplies, always having time to answer technical questions. When he finally went out of business in 2016, this very specially named box was the last one to leave the shop.

If you've spotted something that has "2600" in it or anything else of interest to the hacker world (such as funny uses of "hacker," "unix," "404," you get the idea...), take a picture and send it on in! Be sure to use the highest quality settings on your camera to increase the odds of it getting printed. Make sure and tell us where you spotted your subject along with any other info that makes it interesting - many photos are eliminated due to lack of detail.

Email your submissions to articles@2600.com or use snail mail to *2600* Editorial Dept., PO Box 99, Middle Island, NY 11953 USA.

If we use your picture, you'll get a free one-year subscription (or back issues) and a *2600* t-shirt of your choice.